James E. Cecchi
CARELLA, BYRNE, CECCHI BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700

Interim Lead Class Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: SAMSUNG CUSTOMER DATA SECURITY BREACH LITIGATION	Civil Action No. 23-md-3055 (CPO)(EAP) MDL No. 3055 **AMENDED CONSOLIDATED COMPLAINT AND DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

Plaintiffs Erica Fletcher ("Alabama Plaintiff"); Joshua Fritz ("Alaska Plaintiff"); Todd Bingham ("Arizona Plaintiff"); Jacob Smith ("Arkansas Plaintiff"); Frank Applegate, Brian Heinz, Raffi Kelechian, and Naeem Seirafi ("California Plaintiffs"); Christian Murphy and Jason Vandewater ("Colorado Plaintiffs"); Paul DiGiovanni ("Connecticut Plaintiff"); Matthew McIntyre ("Florida Plaintiff"); Darren Glean ("Georgia Plaintiff"); Eric Carthan, Paris Gardner, Cecilia Tomasevich, and Angelina Alvarado Scott ("Illinois Plaintiffs"); Peggy Rodriguez and Jeremy Dengler ("Indiana Plaintiffs"), Jeremy Collins ("Iowa Plaintiff"); Harold Nyanjom ("Kansas Plaintiff"); Nancy Helis ("Louisiana Plaintiff"); Donald Curtis (Maryland); Carolyn Peavy ("Massachusetts Plaintiff"); Keanna Cole ("Michigan Plaintiff"); Kathleen Shamp ("Minnesota Plaintiff"); Jay Gelizon ("Nevada Plaintiff"); Holly Dorso ("New Hampshire Plaintiff"); Andrew Becker, Amanda Malota, and Joseph Rollins ("New Jersey Plaintiffs"); Indea Sanchez ("New Mexico Plaintiff"); Heather Childs and Michael Ortiz ("New York Plaintiffs"); Katherine Harris ("North Carolina Plaintiff"); Tonisha Jordan and Gina Triola ("Ohio Plaintiffs"); Ronald Allen ("Oklahoma Plaintiff"); Nathan Briggs ("Oregon Plaintiff"); Kristy Capanelli ("Pennsylvania Plaintiff"); Derek Pacheco ("Rhode Island Plaintiff"); Seledia Serina ("South Carolina Plaintiff"); Jamie Barnes, LaShanna Beasley, and Lorinda Hale ("Tennessee Plaintiffs"); Aisha Suleiman ("Texas Plaintiff"); Patel Pratikkumar and Oliver Plummer ("Washington Plaintiffs"); and Steven Baker ("Wisconsin Plaintiff"); individually and on behalf of all others similarly situated, through the undersigned counsel below, hereby allege the following against Defendant Samsung Electronics America, Inc. ("Samsung" or "Defendant"). Based upon personal knowledge as to their own actions, and upon information, belief, and investigation of counsel as to all other matters, Plaintiffs specifically allege as follows:

SUMMARY OF THE CASE

1. Plaintiffs bring this class action on behalf of a nationwide class and statewide sub-classes in 34 states (together, the "Classes") against Samsung for its failure to properly secure and safeguard the sensitive and confidential personally identifiable information, including, but not limited to, full names, email addresses, postal addresses, telephone numbers, dates of birth, Social Security numbers, payment card information, demographic information, and geolocation data (collectively, "personally identifiable information" or "PII"), of millions of its current and former customers ("Class Members").

2. On September 2, 2022, Samsung disclosed that in July 2022, an unauthorized third party exfiltrated and stole a large quantity of PII entrusted to Samsung by its customers (the "Data Breach"), subjecting Plaintiffs and Class Members to not only ongoing and imminent threats of identity theft and fraud, but a heightened and real risk to their personal privacy and safety. Indeed, the geolocation data that Samsung failed to protect included information to determine Plaintiffs' and Class Members' precise locations, as well as their daily routines and associations—information that can be used by bad actors (such as burglars and stalkers) to maliciously target Plaintiffs, Class Members, and their families.

3. The Data Breach was just one in a string of recent data breaches attributable to Samsung's lax data security practices:

- In May 2019, a security researcher discovered that Samsung's internal coding projects were being exposed on an open-source code repository because they lacked proper protection, leaving major Samsung applications open to malicious attacks.
- In February 2020, a glitch occurred in certain Samsung smartphones that allowed some users the ability to access sensitive information belonging to other Samsung

users.

- Just three months later, in May 2020, researchers discovered a "critical security vulnerability" in Samsung smartphones sold from 2014 to 2020 that allowed hackers to penetrate and install malicious code on the phones without any interaction from the phone's owner.
- And, in March 2022, Samsung confirmed that an organization called Lapsus$ had illegally accessed and stolen the source code for Samsung's Galaxy phones and published 190GBs of Samsung's confidential data online.

4. In addition to experiencing its own repeated security breaches, Samsung has, no doubt, been aware of the increasing number of well-publicized data breaches that have occurred in the United States, including several involving Samsung's largest competitors like LG, Sony, and HTC. Yet Samsung utterly failed to properly secure and upgrade its systems, allowing another breach to occur, this time compromising consumer PII.

5. Samsung's data security vulnerabilities have apparently continued unabated since the July 2022 data breach. In December 2022, professional hackers successfully hacked into a Samsung smartphone during a hacking event.[1] And just recently, in April 2023, Samsung disclosed that its own employees had unintentionally leaked sensitive information to ChatGPT.[2]

6. Plaintiffs and Class Members entrusted Samsung with their sensitive and valuable

[1] Davey Winder, Forbes, "Zero-Day Hackers Breach Samsung Galaxy S22 Twice in 24 Hours" (Dec. 7, 2022), available at https://www.forbes.com/sites/daveywinder/2022/12/07/zero-day-hackers-breach-samsung-galaxy-s22-twice-in-24-hours/?sh=5ca8fd5f76ac (last accessed May 19, 2023).

[2] Lewis Maddison, *Samsung workers made a major error by using ChatGPT*, Techradar.Pro, (April 04, 2023), available at https://www.techradar.com/news/samsung-workers-leaked-company-secrets-by-using-chatgpt (last accessed May 19, 2023).

PII. Samsung's actions and omissions are especially egregious because Samsung collected far more PII than it needed to collect from its customers and maintained that data for a far longer period of time than was necessary. Samsung collected and maintained this valuable PII to track its customers and their behaviors, use the data for its own benefit and purposes, and increase its profits.

7. Plaintiffs and Class Members did not know, nor did they have reason to suspect, that Samsung's data security left their PII vulnerable. They did not reasonably expect that by purchasing an electronic device or home appliance or registering for a Samsung account to access device features and use the devices and appliances as Samsung intended, they would suffer serious injury that would last for years after the purchase.

8. Samsung harmed Plaintiffs and Class Members by collecting, using, and maintaining their PII for Samsung's own economic benefit, and then failing to protect that information: Samsung did not maintain proper security systems, did not properly archive the PII, allowed third parties to access the PII, and did not implement proper security measures.

9. Plaintiffs bring this action on behalf of all persons in the United States whose PII was compromised as a result of Defendant's failure to: (i) protect its customers' PII; (ii) warn customers of its inadequate information security practices; and (iii) secure hardware, data, and information systems through compliance with applicable industry standards. Defendant's conduct constitutes negligence and proximately caused damages to Plaintiffs and Class Members.

10. Samsung disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard its customers' PII; failing to take available and necessary steps to prevent unauthorized disclosure of data; and, upon information and belief, failing to follow applicable, required, and

proper protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

11. Alternatively, Defendant has been unjustly enriched. When customers purchase a Samsung Product or Samsung Service (defined below), they are paying for not only the Product or Service itself but proper data management and security as well. Samsung should have invested a greater portion of the monies received from Plaintiffs and Class Members in proper data management and security, including proper and safe storage and disposal of Plaintiffs' and Class Members' PII. Because Defendant failed to implement data management and security measures sufficient to protect that data and comply with industry standards, the principles of equity and justice demand that Defendant not be permitted to retain the money Plaintiffs and Class Members paid Samsung for protection they did not receive.

12. Plaintiffs and Class Members have suffered injuries as a direct and proximate result of Defendant's conduct. These injuries include: (i) lost value of PII, a form of property that Samsung obtained from Plaintiffs and Class Members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their PII; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiffs' and Class Members' unencrypted PII that is available on the dark web; (v) the continued and certain increased risk that the PII that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake proper measures to protect the PII; (v) invasion of privacy and increased risk to personal safety; and (vi) theft of their PII and the resulting

loss of privacy rights in that information.

13. As a direct and proximate result of Samsung's Data Breach and its failure to protect their PII, Plaintiffs and Class Members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, social engineering, and other misuses of their PII, as well as an increased risk to their personal safety; ongoing monetary loss and economic harm, including loss of value of their PII; loss of value of privacy and confidentiality of the stolen PII; illegal sales of the compromised PII; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries. Plaintiffs and Class Members have a continuing interest in ensuring that their personal information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2) because: (1) this is a class action involving more than 100 class members; (2) minimal diversity is present as the Plaintiffs are citizens of thirty-four states (and the proposed class members are from various states) while Defendant is a citizen of New York and New Jersey, and thus Defendant is a citizen of a state different from that of at least one Class Member; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

15. Under 28 U.S.C. § 1332(d)(10), Samsung is a citizen of New York and New Jersey because it is a corporation formed under New York law with its principal place of business in Ridgefield Park, New Jersey.

16. This Court has personal jurisdiction over Samsung because Samsung is

headquartered in New Jersey and regularly conducts business in and throughout New Jersey, and the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues. Samsung has intentionally availed itself of this Court's jurisdiction by conducting operations here, contracting with companies in this District, and marketing and selling its products and services in New Jersey.

17. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to the claims occurred in Ridgefield, New Jersey; and (2) 28 U.S.C. § 1391(b)(3) in that Defendant is subject to personal jurisdiction in this District.

INJURY TO PLAINTIFFS AND CLASS MEMBERS

18. Plaintiffs are individuals whose PII was compromised in the Data Breach. They bring this action on behalf of themselves and all those similarly situated across the United States. Plaintiffs make the following averments upon personal information as to themselves and their experiences and, as to the other averments, upon information and belief, derived from public sources and investigations of their counsel.

19. Because Samsung has exclusive knowledge of the precise information that was compromised for each individual Class Member, Plaintiffs reserve the right to supplement their allegations with additional facts and injuries as they are discovered.

20. Each and every Plaintiff has suffered actual injury and one or more of the concrete (real and not abstract), imminent, and particularized injuries described below as a direct and proximate result of Samsung's known deficient data security and failure to protect Plaintiffs' PII, as well as Samsung's concealment of the same, that allowed unauthorized access to Plaintiffs' PII.

21. Had Samsung disclosed that it had disregarded its duty to protect Plaintiffs' PII or otherwise had insufficient security measures to safeguard and protect Plaintiffs' PII from unauthorized access, Plaintiffs would have taken this into account in making their purchasing decisions.

22. Had Plaintiffs and the Class known that purchasing Samsung Products and Services, creating Samsung accounts, or providing PII to Samsung would result in their PII being compromised and exfiltrated, Plaintiffs and the Class would not have purchased certain products from Samsung, would have paid less for the products or services they bought from Samsung, and/or would not have provided some or all of their PII to Samsung. Thus, Plaintiffs and the Class significantly overpaid based on what Defendant represented the Samsung Products and Services to be, compared to the Samsung products and services Plaintiffs and the Class actually received from Defendant.

23. In addition to the actual, present, concrete, and current injuries described below, because of Samsung's actions and omissions, each and every Plaintiff has suffered, and will continue to suffer perpetual emotional distress, worry, and other emotional or psychological harm, as well as the well-founded fear that additional, realistic, objectively reasonable, threatened, impending, sufficiently imminent harm in the form of identity theft or fraud will occur in the future.

24. As described below for each individual Plaintiff, Plaintiffs have invested, and will continue indefinitely to invest, time and money into precautionary measures that *could*, but may not successfully, mitigate the potential misuse of their data that was compromised in the Data Breach.

25. The Data Breach was the product of an intentional, but avoidable, criminal act to gain access to the data. It was the result of a sophisticated and malicious attack by professional

cybercriminal hackers and was not the result of an accidental disclosure by a Samsung employee. Thus, there is an increased and substantial risk that the victims will experience identity theft or fraud that is sufficiently imminent.

26. Upon information and belief, the PII stolen in the Data Breach included information such as customers' full names, email addresses, postal addresses, telephone numbers, email addresses, dates of birth, Social Security numbers, payment card information, demographic information, and geolocation data, that thieves are likely to use to perpetrate identity theft or fraud, and compromise customers' privacy and security, now or at any time in the future.

27. The concrete injury suffered by Plaintiffs and the Class includes traditional harms such as monetary harm and privacy violations recognized as a basis for a lawsuit in American courts.

28. Plaintiffs have also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of their PII, as well as personal safety risks, resulting in ongoing monetary loss and economic harm, as well as loss of value of PII, loss of value of privacy and confidentiality of the stolen PII, and illegal sales of the compromised PII; mitigation expenses, including identity theft insurance and credit monitoring services; time spent monitoring accounts, initiating and responding to fraud alerts, implementing and removing credit freezes, and contacting third parties; decreased credit scores; and lost work time.

29. The Dark Web is a portion of the internet that facilitates criminal activity worldwide and functions as an underground illicit market for the sale of sensitive stolen data and illegal products such as drugs, weapons, and counterfeit money.

30. There are strong indications that the PII exfiltrated from Samsung's network has been offered for sale on underground marketplaces around the world since late 2022, and that

variations of resells have been occurring ever since.

31. As a result of the Data Breach, Plaintiffs and the Class have been victims of social engineering, including receiving a high-volume of phishing emails and spam telephone calls. Such scams trick consumers into giving account information, passwords, and other valuable personal information to scammers. This significantly increases the risk of further substantial damage to Plaintiffs and the Class, including, but not limited to, monetary and identity theft.

32. Plaintiffs have spent significant time and effort researching the Data Breach, monitoring their accounts for fraudulent activity, reviewing unsolicited emails and texts, and answering unwanted telephone calls. Plaintiffs' and Class Members' awareness of their ongoing, long term, substantial risk for identity theft, and heightened risk to personal safety, has caused emotional distress.

THE PARTIES

A. Plaintiffs

ALABAMA

Erica Fletcher

33. Plaintiff Erica Fletcher is, and was at all relevant times, a citizen and resident of the state of Alabama. Plaintiff Fletcher purchased a Samsung Galaxy A53 on approximately July 11, 2022. In connection with that purchase, Samsung gathered Plaintiff Fletcher's PII.

34. On September 2, 2022, Plaintiff Fletcher received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Fletcher suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Fletcher suffered attempted fraud related to, among other things, scam debt consolidation, misuse of her PII on Instagram, and a

perceptible increase in scams/phishing emails, text messages and/or phone calls. After the Data Breach, Plaintiff Fletcher purchased credit monitoring from Apex Credit Protection. Apex informed Plaintiff Fletcher that her PII is being sold by a third party.

35. Since learning about the Data Breach, Plaintiff Fletcher has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Apex Credit Protection. To date, Plaintiff Fletcher has spent approximately an hour a day checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Fletcher will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Fletcher has also spent approximately $19.99 per month on credit and identity theft protection to protect herself from harm resulting from the Data Breach. Plaintiff Fletcher values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Fletcher been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Fletcher would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Fletcher relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Fletcher has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Fletcher anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

ALASKA

Joshua Fritz

36. Plaintiff Joshua Fritz is, and was at all relevant times, a citizen and resident of the state of Alaska. Plaintiff Fritz purchased three Samsung Galaxy S20 smartphones and two Samsung Smart Watches in approximately 2015. Plaintiff Fritz also purchased a Samsung Smart Television in approximately December 2016. In or around December 2019, he purchased a third Samsung Smart Watch. In connection with these purchases, Samsung gathered Plaintiff Fritz's PII.

37. On September 2, 2022, Plaintiff Fritz received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Fritz suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Fritz suffered an increase in spam calls, and notifications and alerts from the credit monitoring system he uses (AT&T Advanced Mobile Security).

38. Since learning about the Data Breach, Plaintiff Fritz has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and continuing credit monitoring services through AT&T Advanced Mobile Security and CreditWise. Since the Data Breach, Plaintiff Fritz also changed his bank account information and replaced his credit and debit cards. To date, Plaintiff Fritz has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Fritz will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Fritz has spent approximately $10 per month on AT&T Advanced Mobile Security for credit and identity

theft protection. Plaintiff Fritz values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Fritz been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Fritz would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Fritz relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Fritz has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Fritz anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

ARIZONA

Todd Bingham

39. Plaintiff Todd Bingham is, and was at all relevant times, a citizen and resident of the state of Arizona. Over the past five years, Plaintiff Bingham purchased several Samsung cell phones, including a Z-Fold, Galaxy 7, and an A model. In connection with these purchases, Samsung gathered Plaintiff Bingham's PII.

40. On or about September 2, 2022, Plaintiff Bingham received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Bingham suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Bingham suffered fraud and misuse of his PII, including unauthorized charges on his account. As a result of this

fraud, Plaintiff Bingham spent time reversing the charges, cancelling accounts, and changing passwords.

41. Since learning about the Data Breach, Plaintiff Bingham has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Credit Versio. To date, Plaintiff Bingham has spent about a half hour per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Bingham will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Bingham has spent approximately $24.95 per month on the Credit Versio credit monitoring and credit repair service to protect himself from harm resulting from the Data Breach. Plaintiff Bingham values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Bingham been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Bingham would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Bingham relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Bingham has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Bingham anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

ARKANSAS

Jacob Smith

42. Plaintiff Jacob Smith is, and was at all relevant times, a citizen and resident of the state of Arkansas. Plaintiff Smith has purchased at least four Samsung Galaxy phones over a span of years, with some of these purchases occurring as recently as 2021. In connection with these purchases, Samsung gathered Plaintiff Smith's PII.

43. On September 2, 2022, Plaintiff Smith received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Smith suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Smith suffered fraud in the form of ten unauthorized charges on his Samsung Sofi Mastercard totaling $1,000. As a result of the fraud, Plaintiff Smith has spent time and money running fraud searches on identity theft websites.

44. Since learning about the Data Breach, Plaintiff Smith has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Equifax. To date, Plaintiff Smith has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Smith will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Smith has spent approximately $400 to protect himself from harm resulting from the Data Breach. Plaintiff Smith values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Smith been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally,

Plaintiff Smith would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Smith relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Smith has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Smith anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

CALIFORNIA

Frank Applegate

45. Plaintiff Frank Applegate is, and was at all relevant times, a citizen and resident of the state of California. Plaintiff Applegate has been purchasing Samsung products for twenty years. Plaintiff Applegate has purchased a Samsung Galaxy 9, a Galaxy 10, and a Galaxy S20 Ultra. He has also purchased multiple Samsung televisions, a Samsung TV+, and the Samsung Smart Home Audio System. He has also purchased a Samsung Watch and Samsung headphones. In connection with these purchases, Samsung gathered Plaintiff Applegate's PII.

46. On September 2, 2022, Plaintiff Applegate received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. At around the same time, Credit Karma also notified him that his PII had been impacted in the Data Breach. After July 2022, Plaintiff Applegate suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Applegate suffered fraud in connection with unauthorized charges on his account, which caused him to spend time canceling his card, ordering a new card, and making sure the charges were reimbursed. Plaintiff Applegate

has also experienced a perceptible increase in scam/phishing emails, text messages, and/or phone calls, including emails regarding fake loan offers in his name being accepted and approved. Each time he receives these fraudulent emails he is forced to spend time ensuring that no loans are being disbursed in his name. Plaintiff Applegate has also suffered an increase in phishing emails and phone calls about winning lotteries which he did not enter.

47. Since learning about the Data Breach, Plaintiff Applegate has taken precautions to mitigate the risk of future identity theft and fraud, including utilizing the search engine Duck Duck Go; frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Credit Karma. To date, Plaintiff Applegate has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Applegate will need to continue indefinitely to protect against fraud and identity theft. Had Plaintiff Applegate been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Applegate would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Applegate values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Plaintiff Applegate relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Applegate has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Applegate anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Brian Heinz

48. Plaintiff Brian Heinz is, and was at all relevant times, a citizen and resident of the state of California. Plaintiff Heinz purchased a Galaxy Tabs7+ tablet in December 2019. In connection with this purchase, Samsung gathered Plaintiff Heinz's PII.

49. On September 2, 2022, Plaintiff Heinz received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Heinz suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Heinz suffered fraud in the form of unauthorized charges on his debit card and a perceptible increase in scam/phishing emails, text messages, and/or phone calls. As a result of the fraud, Plaintiff Heinz spent time disputing the charges and reviewing his accounts.

50. Since learning about the Data Breach, Plaintiff Heinz has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity and reporting suspicious charges for reimbursement. To date, Plaintiff Heinz has spent roughly 40 hours checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Heinz will need to continue to protect against fraud and identity theft. Plaintiff Heinz values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Heinz been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Heinz would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Heinz relied on Samsung's policies and promises to implement sufficient measures to

protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Heinz has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Heinz anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Raffi Kelechian

51. Plaintiff Raffi Kelechian is, and was at all relevant times, a citizen and resident of the state of California. On or about July 19, 2022, Plaintiff Kelechian purchased a Samsung S22 Ultra phone. In or around 2021, Plaintiff Kelechian also purchased an S21 Ultra phone, a Note 20 Ultra, and a Samsung Galaxy Watch 1. In connection with these purchases, Samsung gathered Plaintiff Kelechian's PII.

52. On September 2, 2022, Plaintiff Kelechian received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Kelechian suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Kelechian has suffered a perceptible increase in scam/phishing emails, text messages, and/or phone calls, and he was notified by Experian that his PII was for sale on the Dark Web.

53. Since learning about the Data Breach, Plaintiff Kelechian has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Experian. To date, Plaintiff Kelechian has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Kelechian will need to continue indefinitely to

protect against fraud and identity theft. Since September 16, 2022, Plaintiff Kelechian has spent approximately $24.99 per month on Experian credit monitoring to protect himself from harm resulting from the Data Breach. Plaintiff Kelechian values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Kelechian been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Kelechian would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Kelechian has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Kelechian anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Naeem Seirafi

54. Plaintiff Naeem Seirafi is, and was at all relevant times, a citizen and resident of the state of California. In or around 2018, Plaintiff Seirafi purchased two Samsung model SCX3400 smart multifunction printers. Plaintiff Seirafi also uses a Samsung application, called Mobile Print, which syncs to his phone. In connection with these purchases, Samsung gathered Plaintiff Seirafi's PII.

55. On September 2, 2022, Plaintiff Seirafi received a data breach notification letter from Samsung by email. After July 2022, Plaintiff Seirafi suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, in July 2022, Plaintiff Seirafi suffered identity theft, fraud, and misuse of his personal information when his

email account was hacked and his phone number stolen in an attempt to hijack his Crypto account. As a result of the Data Breach, Plaintiff Seirafi has spent time and money to secure his information, including putting his email on two secure Ubikey USB hard drives which cost a total of $130.

56. Since learning about the Data Breach, Plaintiff Seirafi has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Credit Karma and Experian. To date, Plaintiff Seirafi has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Seirafi will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Seirafi has spent approximately $130 per month on data security to protect himself from harm resulting from the Data Breach. Plaintiff Seirafi values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Seirafi been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Seirafi would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Seirafi relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Seirafi has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Seirafi anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

COLORADO

Cristian Murphy

57. Plaintiff Cristian Murphy is, and was at all relevant times, a citizen and resident of the state of Colorado. Plaintiff Murphy purchased a Samsung Galaxy Note 9 smartphone in 2017, an S22 smartphone in February 2022, and a Galaxy Watch 3, Samsung TV Series 8, and an S6 Lite tablet over the span of several years. In connection with these purchases, Samsung gathered Plaintiff Murphy's PII.

58. On September 2, 2022, Plaintiff Murphy received a data breach notification letter from Samsung by text message, notifying him that his PII had been compromised in the Data Breach. After July 2022, Plaintiff Murphy suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Murphy suffered fraud in the form of unauthorized charges on one of his credit cards. As a result of this fraud, Plaintiff Murphy has spent approximately 36 hours disputing charges, monitoring and freezing his accounts, and changing passwords and checking credit reports for unapproved lines of credit.

59. Since learning about the Data Breach, Plaintiff Murphy has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Experian and TransUnion. To date, Plaintiff Murphy has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Murphy will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Murphy has spent approximately $300 to protect himself from harm resulting from the Data Breach. Plaintiff Murphy values his privacy and is very concerned about identity theft and the consequences of such theft and fraud

resulting from the Data Breach. Had Plaintiff Murphy been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Murphy would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Murphy relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Murphy has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Murphy anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Jason Vandewater

60. Plaintiff Jason Vandewater is a current resident of Georgia, but lived in Colorado at the time the Data Breach was announced by Samsung. Plaintiff Vandewater has purchased numerous Samsung products over the past twenty years. Before July 2022, Plaintiff Vandewater purchased a Samsung cell phone, 4 Samsung televisions, Samsung headphones, and a Samsung laptop. In connection with these purchases, Samsung gathered Plaintiff Vandewater's PII.

61. On September 2, 2022, Plaintiff Vandewater received a data breach notification letter from Samsung by email. After July 2022, Plaintiff Vandewater suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Vandewater suffered fraud in connection with unauthorized charges on his credit and debit card accounts. As a result of the fraud, Plaintiff Vandewater spent time canceling his cards, ordering new cards, and making sure the charges were reimbursed.

62. Since learning about the Data Breach, Plaintiff Vandewater has taken precautions

to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Experian. To date, Plaintiff Vandewater has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Vandewater will need to continue indefinitely to protect against fraud and identity theft. Since August 2022, Plaintiff Vandewater has spent approximately $9.99 per month on Experian credit monitoring services to protect himself from harm resulting from the Data Breach. Plaintiff Vandewater values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Vandewater been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Vandewater would not have purchased the above-mentioned Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Vandewater relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Vandewater has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Vandewater anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

CONNECTICUT

Paul DiGiovanni

63. Plaintiff Paul DiGiovanni is, and was at all relevant times, a citizen and resident of the state of Connecticut. In or around April 2022, Plaintiff DiGiovanni purchased a Samsung cell

phone. Over the course of time, Plaintiff DiGiovanni has also purchased the following Samsung products: a refrigerator, Galaxy cell phones, tablets, televisions, a microwave, a robot vacuum, a laptop, and a stereo system. In connection with these purchases, Samsung gathered Plaintiff DiGiovanni's PII.

64. On September 2, 2022, Plaintiff DiGiovanni received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff DiGiovanni suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, in or about September 2022 and February 2023, Plaintiff DiGiovanni suffered from identity theft when several fraudulent accounts were opened in his name and he received a fraudulent hospital bill in his name. As a result of these instances of identity theft, Plaintiff DiGiovanni has spent time cancelling and/or freezing accounts, disputing charges, and changing passwords.

65. Since learning about the Data Breach, Plaintiff DiGiovanni has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity and obtaining and reviewing credit bureau reports. To date, Plaintiff DiGiovanni has spent about an hour per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff DiGiovanni will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff DiGiovanni has spent approximately $40 per month on Norton credit monitoring to protect himself from harm resulting from the Data Breach. Plaintiff DiGiovanni values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff DiGiovanni been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions.

Additionally, Plaintiff DiGiovanni would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff DiGiovanni relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff DiGiovanni has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff DiGiovanni anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

FLORIDA

Matthew McIntyre

66. Plaintiff Matthew McIntyre is, and was at all relevant times, a citizen and resident of the state of Florida. Plaintiff McIntyre has purchased a number of Samsung products. In early 2021, Plaintiff McIntyre purchased a Samsung Note 10+. In addition, since 2020, he has purchased a Z-Fold 3 smartphone, a Z-Fold 4 smartphone, Samsung Z3 tablet Earbuds and the Live Edition of the Earbuds, a 65" curved Smart TV, and a sound system. In connection with these purchases, Samsung gathered Plaintiff McIntyre's PII.

67. On September 2, 2022, Plaintiff McIntyre received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff McIntyre suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, between October 2022 and March 2023, Plaintiff McIntyre has suffered identity theft and fraud in the form of a fraudulent loan taken out in his name, fraudulent charges on his debit card amounting to over $600, and over 120 credit inquiries under his name. As a result of this identity theft and fraud, Plaintiff McIntyre has spent

time disputing charges, cancelling accounts, and changing passwords.

68. Since learning about the Data Breach, Plaintiff McIntyre has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; instituting a credit freeze; and obtaining and/or continuing credit monitoring services through Verizon. To date, Plaintiff McIntyre has spent at least 60 hours checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff McIntyre will need to continue to protect against fraud and identity theft. As of this filing, Plaintiff McIntyre has spent approximately $10 per month on Verizon identity protection and over $200 pulling his credit reports to protect himself from harm resulting from the Data Breach. Plaintiff McIntyre values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff McIntyre been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff McIntyre would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff McIntyre relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff McIntyre has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff McIntyre anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

GEORGIA

Darren Glean

69. Plaintiff Darren Glean is, and was at all relevant times, a citizen and resident of the state of Georgia. Plaintiff Glean has purchased numerous Samsung products over the span of years including a Galaxy 10E in 2019 and a Galaxy S21 in 2021. In connection with these purchases, Samsung gathered Plaintiff Glean's PII.

70. On September 2, 2022, Plaintiff Glean received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Glean suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Glean has suffered fraud in the form of unauthorized charges on his credit cards and the misuse of his PII, including a perceptible increase in scam/phishing phone calls. As a result of the fraud and misuse, Plaintiff Glean has spent nearly 100 hours fielding spam calls, conducting internet research, and calling various agencies to get more information on how his information is being misused.

71. Since learning about the Data Breach, Plaintiff Glean has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; and obtaining and reviewing credit bureau reports. To date, Plaintiff Glean has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Glean will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Glean values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Glean been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally,

Plaintiff Glean would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Glean relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Glean has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Glean anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

ILLINOIS

Eric Carthan

72. Plaintiff Eric Carthan is, and was at all relevant times, a citizen and resident of the state of Illinois. Since July 2021, Plaintiff Carthan purchased a Samsung Galaxy 22 Ultra and a Galaxy Z Fold 4 cell phone, a Samsung Galaxy Book 2 Pro 360 laptop, a Samsung Galaxy Watch 5, two Samsung televisions (65 Inch Class QN Neeo QLED and 43 Inch Class QN Samsung Neo QLED 4K Smart TV), and a Galaxy tablet S8 Plus. In connection with these purchases, Samsung gathered Plaintiff Carthan's PII.

73. On September 2, 2022, Plaintiff Carthan received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Carthan suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Carthan has suffered identity theft and fraud, in the form of unauthorized charges and purchases he did not make. As a result of this identity theft and fraud, Plaintiff Carthan has spent numerous hours disputing charges, cancelling accounts, and changing passwords.

74. Since learning about the Data Breach, Plaintiff Carthan has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services. To date, Plaintiff Carthan has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Carthan will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Carthan has spent approximately $23 per month on LifeLock, MacAfee virus protection, and Express VPN to protect himself from harm resulting from the Data Breach. Plaintiff Carthan values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Carthan been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Plaintiff Carthan would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Carthan relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Carthan has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Carthan anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Paris Gardner

75. Plaintiff Paris Gardner is, and was at all relevant times, a citizen and resident of the state of Illinois. In or about 2022, Plaintiff Gardner purchased a Samsung S22+ cell phone, Samsung Galaxy tablet, Samsung Galaxy Tab laptop, and Galaxy 5 Watch Pro. Prior to 2022,

Plaintiff Gardner purchased the following: Note 20, Note 10, Note 8, Note 5, S-3, S-2, mini tablets, and Samsung TV. In connection with these purchases, Samsung gathered Plaintiff Gardner's PII.

76. On or about September 2, 2022, Plaintiff Gardner received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Gardner suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Gardner has suffered identity theft in the form of unauthorized openings of email accounts in his name. As a result of this identity theft, Plaintiff Gardner has spent time changing passwords and monitoring his accounts.

77. Since learning about the Data Breach, Plaintiff Gardner has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through McAfee. To date, Plaintiff Gardner has spent about an hour per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Gardner will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Gardner has spent approximately $15 on a credit freeze to protect himself from harm resulting from the Data Breach. Plaintiff Gardner values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Gardner been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Gardner would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Gardner relied on Samsung's policies and promises to implement sufficient

measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Gardner has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Gardner anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Angelina Alvarado Scott

78. Plaintiff Angelina Alvarado Scott is, and was at all relevant times, a citizen and resident of the state of Illinois. In or about May 2020, Plaintiff Scott purchased a Samsung Galaxy Watch and a Galaxy Note+. She purchased a Samsung Smart TV in March 2021 and a Samsung Tablet in April 2021. In connection with these purchases, Samsung gathered Plaintiff Scott's PII.

79. On September 2, 2022, Plaintiff Scott received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Scott suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, starting in or about August 2022, Plaintiff Scott has suffered payment account fraud and a perceptible increase in scam/phishing emails and text messages. As a result of the payment account fraud, Plaintiff Scott spent approximately 10 hours changing accounts and passwords.

80. Since learning about the Data Breach, Plaintiff Scott has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Credit Karma, Credit Sesame, and a paid service from Experian. To date, Plaintiff Scott has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Scott will

need to continue indefinitely to protect against fraud and identity theft. Plaintiff Scott spent approximately $24.99 per month in January and February 2023 on Experian to protect herself from harm resulting from the Data Breach. Plaintiff Scott values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Scott been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Scott would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Scott relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Scott has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Scott anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Cecilia Tomasevich

81. Plaintiff Cecilia Tomasevich is, and was at all relevant times, a citizen and resident of the state of Illinois. In or about March 2021, Plaintiff Tomasevich purchased a Samsung S7+ tablet. Plaintiff Tomasevich previously purchased numerous other Samsung products including a Smart TV, earphones, and smartphone. In connection with these purchases, Samsung gathered Plaintiff Tomasevich's PII.

82. On September 2, 2022, Plaintiff Tomasevich received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Tomasevich suffered injury and was damaged as a result of Samsung's

failure to keep her PII secure. As a result of the Data Breach, in September 2022, Plaintiff Tomasevich suffered fraud in the form of unauthorized charges on her credit card. As a result of the credit card fraud, Plaintiff Tomasevich has spent time disputing the charges, reviewing and monitoring her accounts, and changing her passwords.

83. Since learning about the Data Breach, Plaintiff Tomasevich has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Discover and Chase Bank. To date, Plaintiff Tomasevich has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Tomasevich will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Tomasevich values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Tomasevich been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Tomasevich would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Tomasevich relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Tomasevich has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Tomasevich anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

INDIANA

Jeremy Dengler

84. Plaintiff Jeremy Dengler is, and was at all relevant times, a citizen and resident of the state of Indiana. On or about March 20, 2021, Plaintiff Dengler purchased a Samsung Galaxy S21 Ultra phone. On or about November 28, 2019, Plaintiff Dengler also purchased a Samsung Chromebook. On or about October 4, 2018, Plaintiff Dengler also purchased a Galaxy Note 9. In connection with these purchases, Samsung gathered Plaintiff Dengler's PII.

85. On September 2, 2022, Plaintiff Dengler received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Dengler suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Dengler has suffered fraud in the form of unauthorized charges that were reported on his credit report and a perceptible increase in scam/phishing emails, text messages, and phone calls. As a result of this fraud, Plaintiff Dengler spent time disputing the charges and changing passwords on his accounts.

86. Since learning about the Data Breach, Plaintiff Dengler has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; requesting and unlocking credit freezes, obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Credit Karma and Experian. To date, Plaintiff Dengler has spent about 12 hours checking his credit and financial accounts for any unauthorized activity, addressing and disputing the fraudulent charges, and changing passwords, which are practices that Plaintiff Dengler will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Dengler has spent approximately $40 on McAfee virus protection and security suite to protect

himself from harm resulting from the Data Breach. Plaintiff Dengler values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Dengler been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Dengler would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Dengler relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Dengler has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Dengler anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Peggy Rodriguez

87. Plaintiff Peggy Rodriguez is, and was at all relevant times, a citizen and resident of the state of Indiana. In April 2018, Plaintiff Rodriguez purchased a Samsung Galaxy S20. In April 2020, she purchased a Galaxy S21, and, in April 2022, a Galaxy S22. Plaintiff Rodriguez also purchased two Galaxy Tab8 tablets in December 2021. In connection with these purchases, Samsung gathered Plaintiff Rodriguez's PII.

88. On September 2, 2022, Plaintiff Rodriguez received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Rodriguez suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Rodriguez suffered identity theft and fraud in the form of an unauthorized charge on her Comcast Xfinity account, the unauthorized

opening of an email account in her name, and two fraudulent charges on her debit card in the amounts of $135 and $200 purportedly from Michigan Lottery. As a result of the identity theft and fraud, Plaintiff Rodriguez spent time disputing charges, cancelling accounts, and changing passwords.

89. Since learning about the Data Breach, Plaintiff Rodriguez has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity and freezing her credit. To date, Plaintiff Rodriguez has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Rodriguez will need to continue to protect against fraud and identity theft. Plaintiff Rodriguez values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Rodriguez been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Rodriguez would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Rodriguez relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Rodriguez has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Rodriguez anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

IOWA

Jeremy Collins

90. Plaintiff Jeremy Collins is, and was at all relevant times, a citizen and resident of the state of Iowa. On average, since 2012, Plaintiff Collins has purchased a Samsung cell phone every other year, including the following: Galaxy S20, Galaxy 832 5G, Galaxy 851, Galaxy Tab A 32 Gig, Galaxy S22 Ultra, all the way back to the Galaxy 3. In connection with these purchases, Samsung gathered Plaintiff Collins' PII.

91. On or about September 2, 2022, Plaintiff Collins received a data breach notification letter from Samsung by email. After July 2022, Plaintiff Collins suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Collins has suffered a perceptible increase in scam/phishing emails, text messages, and phone calls. As a result of this increase, Plaintiff Collins has spent time fielding scam/phishing communications and maintaining his communication accounts.

92. Since learning about the Data Breach, Plaintiff Collins has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; and obtaining and reviewing credit bureau reports. To date, Plaintiff Collins has spent about a half hour per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Collins will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Collins values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Collins been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Collins would not have purchased the Samsung products or

services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Collins relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Collins has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Collins anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

KANSAS

Harold Nyanjom

93. Plaintiff Harold Nyanjom is, and was at all relevant times, a citizen and resident of the state of Kansas. In the Fall of 2018, Plaintiff Nyanjom purchased a Samsung Galaxy J4. In the Fall of 2017, Plaintiff Nyanjom also purchased a Samsung Galaxy A737. In connection with these purchases, Samsung gathered Plaintiff Nyanjom's PII.

94. On September 2, 2022, Plaintiff Nyanjom received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Nyanjom suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Nyanjom has suffered fraud and the misuse of his PII in the form of unauthorized charges on his AT&T account and notifications from his CreditWise and CreditKarma accounts that his PII was being misused. As a result of this fraud and misuse, Plaintiff Nyanjom spent time disputing charges and changing passwords.

95. Since learning about the Data Breach, Plaintiff Nyanjom has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and

continuing credit monitoring services through CreditWise and CreditKarma. To date, Nyanjom has spent at least an hour per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Nyanjom will need to continue to protect against fraud and identity theft. Plaintiff Nyanjom values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Nyanjom been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Nyanjom would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Nyanjom relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Nyanjom has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Nyanjom anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

LOUISIANA

Nancy Helis

96. Plaintiff Nancy Helis is, and was at all relevant times, a citizen and resident of the state of Louisiana. Plaintiff Helis has purchased numerous Samsung products over the past 15 years, including in March 2021, a Samsung Galaxy S21 5G. Before that, Plaintiff Helis purchased a Galaxy S7, which she bought in or around 2014, and a Galaxy S3 in or around 2007. She has also purchased Samsung Smart TVs, computer monitors, tablets, and fitness watches. In connection with these purchases, Samsung gathered Plaintiff Helis's PII.

97. On September 2, 2022, Plaintiff Helis received a data breach notification letter

from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Helis suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, starting on or about July 2022, Plaintiff Helis has suffered a perceptible increase in scam/phishing emails, text messages, and/or phone calls. As a result of the increase in scam/phishing emails, Plaintiff Helis has complained to Microsoft and has forwarded scam/phishing emails to scam baiters in an attempt to lessen the amount of scam/phishing emails she receives. Plaintiff Helis estimates she has spent 200 hours dealing with scam/phishing emails since July 2022.

98. Since learning about the Data Breach, Plaintiff Helis has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; and obtaining and/or continuing credit monitoring services through US Bank. To date, Plaintiff Helis has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Helis will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Helis values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Helis been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Helis would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Helis relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Helis has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the

Data Breach, Plaintiff Helis anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

MARYLAND

Donald Curtis

99. Plaintiff Donald Curtis is, and was at all relevant times, a citizen and resident of the state of Maryland. Plaintiff Curtis purchased a Samsung Note 20 in approximately 2022. He has purchased Samsung cellphones for the last 10 years. In connection with those purchases, Samsung gathered Plaintiff Curtis's PII.

100. On or about September 2, 2022, Plaintiff Curtis received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Curtis suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Curtis suffered identity theft and fraud when he was notified that a credit card was opened in his name on or around February 2023 and that his social security number was used. As a result of this identity theft and fraud, Plaintiff Curtis spent time restoring his identity, monitoring his accounts, and changing his passwords.

101. Since learning about the Samsung Data Breach, Plaintiff Curtis has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity and obtaining and reviewing credit bureau reports. To date, including the time spent restoring his identity, Plaintiff Curtis has spent more than 50 hours checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Curtis will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Curtis values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had he been informed that

Samsung had insufficient data security measures to protect his PII, he would never have purchased a Samsung product or provided his/her PII to Samsung. Plaintiff Curtis relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Curtis has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Curtis anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

MASSACHUSETTS

Carolyn Peavy

102. Plaintiff Carolyn Peavy is, and was at all relevant times, a citizen and resident of the state of Massachusetts. Starting in and around 2018 and continuing through 2022, Plaintiff Peavy purchased a number of Samsung products including a Galaxy S8, Galaxy S10E, Z Flip 3, and a Smart TV. In connection with these purchases, Samsung gathered Plaintiff Peavy's PII.

103. On September 2, 2022, Plaintiff Peavy received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Peavy suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Peavy suffered identity theft when someone stole her exact email address and through the misuse of her personal information in the form of a perceptible increase in scam/phishing emails. Plaintiff Peavy also learned that her information is on the Dark Web. As a result of the identity theft and misuse of her information, Plaintiff Peavy has spent time every day monitoring and managing her email account.

104. Since learning about the Data Breach, Plaintiff Peavy has taken precautions to

mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Credit Wise. To date, Plaintiff Peavy has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Peavy will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Peavy values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Peavy been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Peavy would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Peavy relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Peavy has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Peavy anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

MICHIGAN

Keanna Cole

105. Plaintiff Keanna Cole is, and was at all relevant times, a citizen and resident of the state of Michigan. In or around 2020, Plaintiff Cole purchased a Samsung Galaxy S20. In connection with this purchase, Samsung gathered Plaintiff Cole's PII.

106. On September 2, 2022, Plaintiff Cole received a data breach notification letter from

Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Cole suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Cole suffered misuse of her PII in the form of unauthorized credit inquires, and a perceptible increase in scam/phishing phone calls regarding extending warranties. As a result of the unauthorized credit inquiries and influx of scam/phishing calls, Plaintiff Cole has spent time checking her credit reports and blocking phone numbers.

107. Since learning about the Data Breach, Plaintiff Cole has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Equifax. To date, Plaintiff Cole has spent an hour per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Cole will need to continue indefinitely to protect against fraud and identity theft. To date, Plaintiff Cole has spent approximately $12.99 per month on Equifax to protect herself from harm resulting from the Data Breach. Plaintiff Cole values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Cole been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Cole would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Cole relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Cole has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff

Cole anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

MINNESOTA

Kathleen Shamp

108. Plaintiff Kathleen Shamp is, and was at all relevant times, a citizen and resident of the state of Minnesota. In or around June 9, 2018, Plaintiff Shamp purchased a Samsung Galaxy S6. In or around August 3, 2021, Plaintiff Shamp purchased a Galaxy S21. In connection with these purchases, Samsung gathered Plaintiff Shamp's PII.

109. On September 2, 2022, Plaintiff Shamp received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Shamp suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, in or about July 2022, Plaintiff Shamp suffered identity theft, fraud, and misuse of her personal information when unauthorized credit cards, a small business loan, and a Minnesota tax refund were fraudulently obtained in her name. As a result of this identity theft and fraudulent activity, Plaintiff Shamp has spent over 20 hours disputing the loan and credit applications, freezing her credit, and restoring her identity.

110. Since learning about the Data Breach, Plaintiff Shamp has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Experian. To date, Plaintiff Shamp has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Shamp will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Shamp values her privacy and is very concerned about identity theft

and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Shamp been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Shamp would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Shamp relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Shamp has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Shamp anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

NEVADA

Jay Gelizon

111. Plaintiff Jay Gelizon is, and was at all relevant times, a citizen and resident of the state of Nevada. Plaintiff Gelizon purchased a Samsung Galaxy Note 10+ on January 11, 2020. In connection with that purchase, Samsung gathered Plaintiff Gelizon's PII.

112. On September 2, 2022, Plaintiff Gelizon received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Gelizon suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Gelizon has suffered increased spam or phishing emails and text messages.

113. Since learning about the Data Breach, Plaintiff Gelizon has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and

obtaining and/or continuing credit monitoring services through Credit Karma and Rocket Money. To date, Plaintiff Gelizon has spent approximately 2 hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Gelizon will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Gelizon values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Gelizon been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Gelizon would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Gelizon relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Gelizon has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Gelizon anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

NEW HAMPSHIRE

Holly Dorso

114. Plaintiff Holly Dorso is, and was at all relevant times, a citizen and resident of the state of New Hampshire. About ten years ago, Plaintiff Dorso purchased a Galaxy tablet. Plaintiff Dorso's husband purchased her a Samsung Galaxy S21 in 2021. Plaintiff Dorso also purchased a Samsung Galaxy Watch on April 21, 2021. In connection with these purchases, Samsung gathered Plaintiff Dorso's PII.

115. On September 2, 2022, Plaintiff Dorso received a data breach notification letter

from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Dorso suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Dorso has suffered misuse of her PII and a perceptible increase in scam/phishing emails, text messages and phone calls.

116. Since learning about the Data Breach, Plaintiff Dorso has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Equifax. To date, Plaintiff Dorso has spent 2-3 hours per week checking her credit and financial accounts for any unauthorized activity and dealing with spam and phishing emails and texts, a practice that Plaintiff Dorso will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Dorso values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Dorso been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Dorso would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Dorso relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Dorso has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Dorso anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

NEW JERSEY

Andrew Becker

117. Plaintiff Andrew Becker is, and was at all relevant times, a citizen and resident of the state of New Jersey. Plaintiff Becker purchased two Samsung Galaxy S22 Ultra smartphones in approximately December 2021. Plaintiff Becker also purchased a Samsung Note 8 and Note 6 tablet in approximately December 2021. In connection with that purchase, Samsung gathered Plaintiff Becker's PII.

118. On or about September 2, 2022, Plaintiff Becker received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Becker suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Becker suffered 5 unauthorized charges on his debit card that totaled over $1,000. On or about September 2022, Plaintiff Becker changed his debit card and bank account information due to continued suspicious activity.

119. Since learning about the Data Breach, Plaintiff Becker has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity and changing account information. To date, Plaintiff Becker has spent over 40 hours checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Becker will need to continue to protect against fraud and identity theft. Plaintiff Becker values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Becker been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Becker would not have purchased the Samsung products or services or would have paid less for them and

would have limited the PII provided to Samsung. Plaintiff Becker relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Becker has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Becker anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Amanda Malota

120. Plaintiff Amanda Malota is, and was at all relevant times, a citizen and resident of the state of New Jersey. Plaintiff Malota purchased a Samsung Galaxy S21 Ultra 5G and a Galaxy 10+ in approximately 2019. Plaintiff Malota also purchased Samsung Smart televisions and a Samsung tablet. In connection with these purchases, Samsung gathered Plaintiff Malota's PII.

121. On or about September 2, 2022, Plaintiff Malota received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Malota suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Malota suffered identity theft in the form of fraudulent charges. As a result of the fraudulent charges, Plaintiff Malota spent time and money disputing the charges and correcting the mistakes on her credit report.

122. Since learning about the Data Breach, Plaintiff Malota has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity and obtaining and reviewing credit bureau reports. To date, Plaintiff Malota has spent time checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Malota will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Malota has spent approximately $600

disputing the fraudulent charges and to protect herself from harm resulting from the Data Breach. Plaintiff Malota values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Malota been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Malota would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Malota relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Malota has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Malota anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Joseph Rollins

123. Plaintiff Joseph Rollins is, and was at all relevant times, a citizen and resident of the state of New Jersey. Plaintiff Rollins has purchased numerous Samsung products over the years including a Galaxy S10 and Samsung tablets. In connection with these purchases, Samsung gathered Plaintiff Rollins' PII.

124. On or about September 2, 2022, Plaintiff Rollins received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Rollins suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Rollins suffered misuse of his PII in the form of a perceptible increase in scam/phishing emails, text messages, and phone calls. As a result of this misuse, Plaintiff Rollins has spent time changing passwords, monitoring his

accounts, instituting a credit freeze, reissuing accounts, and fielding phishing scams.

125. Since learning about the Data Breach, Plaintiff Rollins has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit reports; and obtaining and/or continuing credit monitoring services through Capital One. To date, Plaintiff Rollins has spent approximately 5-6 hours checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Rollins will need to continue to protect against fraud and identity theft. Plaintiff Rollins values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Rollins been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Rollins would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Rollins relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Rollins has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Rollins anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

NEW MEXICO

Indea Sanchez

126. Plaintiff Indea Sanchez is, and was at all relevant times, a citizen and resident of the state of New Mexico. In or around 2020, Plaintiff Sanchez purchased a Samsung Galaxy S20 Ultra FE and in or around 2015, she purchased two Samsung televisions. In connection with these

purchases, Samsung gathered Plaintiff Sanchez's PII.

127. On September 2, 2022, Plaintiff Sanchez received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Sanchez suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, on or about September 2022, Plaintiff Sanchez suffered fraud in the form of 6 unauthorized charges on her bank account. As a result of this fraud, Plaintiff Sanchez has spent time disputing the charges and monitoring her accounts.

128. Since learning about the Data Breach, Plaintiff Sanchez has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; and obtaining and reviewing credit bureau reports. To date, Plaintiff Sanchez has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Sanchez will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Sanchez values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Sanchez been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Sanchez would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Sanchez relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Sanchez has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Sanchez anticipates spending considerable time and money on an ongoing basis to

mitigate and address the harms caused by the Data Breach.

NEW YORK

Heather Childs

129. Plaintiff Heather Childs is, and was at all relevant times, a citizen and resident of the state of New York. Plaintiff Childs purchased a Samsung Galaxy 1 Watch in approximately January 2022, and a Galaxy S20 Ultra phone in April 2022. In connection with these purchases, Samsung gathered Plaintiff Childs' PII.

130. On or about September 2, 2022, Plaintiff Childs received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Childs suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Childs suffered attempted fraud including fraudulent invoices and emails from certain companies.

131. Since learning about the Data Breach, Plaintiff Childs has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Chase Bank, Capital One, Norton 360, and McAfee Total Protection. To date, Plaintiff Childs has spent approximately 40 hours addressing fake charges, 5 hours over the course of 5 separate phone calls with Samsung reporting this problem, and approximately 2 hours a week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Childs will need to continue indefinitely to protect against fraud and identity theft. As of this filing, Plaintiff Childs has spent approximately $40 per month, including Norton 360 ($279/year), McAfee ($196/year), Chase ($5/month), Capital One ($6/month) on credit monitoring and identity theft protection to protect herself from harm resulting

from the Data Breach. Plaintiff Childs values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Childs been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Childs would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Childs relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Childs has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Childs anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Michael Ortiz

132. Plaintiff Michael Ortiz is, and was at all relevant times, a citizen and resident of the state of New York. On or about March 2022, Plaintiff Ortiz purchased a Samsung Galaxy A53 phone. In connection with this purchase, Samsung gathered Plaintiff Ortiz's PII.

133. On September 2, 2022, Plaintiff Ortiz received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Ortiz suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Ortiz suffered identity theft. After the Data Breach, Plaintiff Ortiz had to put a block on his Social Security Number and eventually had to get another Social Security card, which took about a month and involved him making a report to the Social Security Administration.

134. Since learning about the Data Breach, Plaintiff Ortiz has taken precautions to

mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; monitoring his credit; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services. To date, Plaintiff Ortiz spends about 2 hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Ortiz will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Ortiz values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Ortiz been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Ortiz would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Ortiz relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Ortiz has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Ortiz anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

NORTH CAROLINA

Katherine Harris

135. Plaintiff Katherine Harris is, and was at all relevant times, a citizen and resident of the state of North Carolina. In or around March 2022, Plaintiff Harris purchased a Samsung Note 20 smartphone and a Galaxy 8 tablet. In connection with these purchases, Samsung gathered Plaintiff Harris' PII

136. On September 2, 2022, Plaintiff Harris received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Harris suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Harris suffered identity theft and misuse of her PII, in the form of credit card fraud. Starting in or about September 2022, Plaintiff Harris was notified of multiple occurrences of fraudulent attempts to open credit cards and apply for a home loan in her name, and has suffered multiple unauthorized charges to her Cash/App account. As a result of this identity theft and fraud, Plaintiff Harris has spent approximately 25-30 hours disputing charges and calling credit companies and agencies to understand who was trying to use her information fraudulently.

137. Since learning about the Data Breach, Plaintiff Harris has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining credit freezes through Equifax, Experian, and TransUnion. To date, Plaintiff Harris has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Harris will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Harris values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Harris been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Harris would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Harris relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly

sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Harris has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Harris anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

OHIO

Tonisha Jordan

138. Plaintiff Tonisha Jordan is, and was at all relevant times, a citizen and resident of the state of Ohio. Plaintiff Jordan purchased a Samsung Galaxy S21 phone in May 2021. In connection with that purchase, Samsung gathered Plaintiff Jordan's PII.

139. On September 2, 2022, Plaintiff Jordan received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Jordan suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Jordan suffered fraud in the form of unauthorized charges on her Paypal account. As a result of this fraud, Plaintiff Jordan spent time disputing the charges, reviewing and monitoring her accounts and changing passwords.

140. Since learning about the Data Breach, Plaintiff Jordan has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Credit Karma. To date, Plaintiff Jordan has spent approximately 3 hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Jordan will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Jordan values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

Had Plaintiff Jordan been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Jordan would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Jordan relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Jordan has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Jordan anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Gina Triola

141. Plaintiff Gina Triola is, and was at all relevant times, a citizen and resident of the state of Ohio. Plaintiff Triola purchased a number of Samsung products including a Galaxy phone in approximately 2012/2013, a Smart TV in December 2016, and a Samsung Galaxy S21 FE in March 2022. In connection with these purchases, Samsung gathered Plaintiff Triola's PII.

142. On September 2, 2022, Plaintiff Triola received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Triola suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Triola experienced a perceptible increase in the amount of spam/phishing emails and text messages. As a result of this increase in scam/phishing emails and text messages, Plaintiff Triola has spent time reviewing and maintaining her communication accounts.

143. Since learning about the Data Breach, Plaintiff Triola has taken precautions to

mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; and obtaining and reviewing credit bureau reports. To date, Plaintiff Triola has spent a couple hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Triola will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Triola values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Triola been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Triola would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Triola relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Triola has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Triola anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

OKLAHOMA

Ronald Allen

144. Plaintiff Ronald Allen is, and was at all relevant times, a citizen and resident of the state of Oklahoma. Plaintiff Allen purchased a Samsung Fold 4 phone, a Samsung Fold 3 phone, and a Samsung Galaxy Watch 2 in 2021. In connection with these purchases, Samsung gathered Plaintiff Allen's PII.

145. On September 2, 2022, Plaintiff Allen received a data breach notification from

Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Allen suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Allen suffered attempted fraud including an attempt to open an account in his name, strange text messages, and emails from his credit card company stating that his credit card information had been found on the Dark Web.

146. Since learning about the Data Breach, Plaintiff Allen has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services. To date, Plaintiff Allen has spent 1-3 hours per week checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Allen will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Allen values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Allen been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Allen would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Allen relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Allen has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Allen anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

OREGON

Nathan Briggs

147. Plaintiff Nathan Briggs is, and was at all relevant times, a citizen and resident of the state of Oregon. Plaintiff Briggs purchased a Samsung Galaxy A02S and a Smart TV 4K in December 2021. In connection with these purchases, Samsung gathered Plaintiff Briggs' PII.

148. On or about September 2, 2022, Plaintiff Briggs received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Briggs suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Briggs suffered identity theft, including fraudulent loan applications in his name as well as fraudulent bills. As a result of this identity theft, Plaintiff Briggs spent time correcting his credit reports and monitoring his accounts.

149. Since learning about the Data Breach, Plaintiff Briggs has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and keeping his credit cards locked. To date, Plaintiff Briggs has spent over 240 hours remediating the instances of identity theft as well as approximately 2 hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Briggs will need to continue indefinitely to protect against fraud and identity theft. To rectify the Verizon identity theft, Plaintiff Briggs spent approximately $110 to protect himself from harm resulting from the Data Breach. Plaintiff Briggs values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Briggs been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Briggs would

not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Briggs relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Briggs has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Briggs anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

PENNSYLVANIA

Kristy Capanelli

150. Plaintiff Kristy Capanelli is, and was at all relevant times, a citizen and resident of the state of Pennsylvania. Plaintiff Capanelli purchased multiple Samsung Galaxy cell phones including an A21, A15 and A103. In connection with these purchases, Samsung gathered Plaintiff Capanelli's PII.

151. On or about September 2, 2022, Plaintiff Capanelli received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Capanelli suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Capanelli suffered fraud, in the form of unauthorized charges on her Direct Express account. As a result of the fraud, Plaintiff Capanelli spent time disputing charges, cancelling accounts, and changing passwords.

152. Since learning about the Data Breach, Plaintiff Capanelli has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and

obtaining and/or continuing credit monitoring services through McAfee. To date, Plaintiff Capanelli has spent about a half hour per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Capanelli will need to continue indefinitely to protect against fraud and identity theft. To date, Plaintiff Capanelli has spent approximately $4 per month on credit monitoring to protect herself from harm resulting from the Data Breach. Plaintiff Capanelli values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Capanelli been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Capanelli would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Capanelli relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Capanelli has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Capanelli anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

RHODE ISLAND

Derek Pacheco

153. Plaintiff Derek Pacheco is, and was at all relevant times, a citizen and resident of the state of Rhode Island. Plaintiff Pacheco purchased a Galaxy S10 in or around 2018 or 2019. In connection with this purchase, Samsung gathered Plaintiff Pacheco's PII.

154. On or about September 2, 2022, Plaintiff Pacheco received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data

Breach. After July 2022, Plaintiff Pacheco suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Pacheco suffered misuse of his PII in the form of an increase in scam/phishing emails, text messages, and phone calls. As a result of this misuse, Plaintiff Pacheco has spent time managing his accounts and fielding scam/phishing communications.

155. Since learning about the Data Breach, Plaintiff Pacheco has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity. To date, Plaintiff Pacheco has spent about a half hour per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Pacheco will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Pacheco values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Pacheco been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Pacheco would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Pacheco relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Pacheco has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Pacheco anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

SOUTH CAROLINA

Seledia Serina

156. Plaintiff Seledia Serina is, and was at all relevant times, a citizen and resident of the state of South Carolina. Starting in or about 2013, Plaintiff Serina purchased several Samsung smart phones including, in or about 2017, a Samsung S9 cell phone. In or about 2020, Plaintiff Serina purchased a Samsung refrigerator. In connection with these purchases, Samsung gathered Plaintiff Serina's PII.

157. On September 2, 2022, Plaintiff Serina received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Serina suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, in or around August 2022, Plaintiff Serina suffered fraud in the form of an unauthorized charge on her bank card. As a result of the fraud, Plaintiff Serina spent time disputing the charge, cancelling her bank card, and monitoring her accounts.

158. Since learning about the Data Breach, Plaintiff Serina has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; and obtaining and reviewing credit bureau reports. To date, Plaintiff Serina has spent approximately an hour each week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Serina will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Serina values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Serina been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her

purchasing decisions. Additionally, Plaintiff Serina would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Serina relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Serina has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Serina anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

TENNESSEE

Jamie Barnes

159. Plaintiff Jamie Barnes is, and was at all relevant times, a citizen and resident of the state of Tennessee. Plaintiff Barnes purchased a Samsung Galaxy 10A in approximately 2018-2019. In connection with that purchase, Samsung gathered Plaintiff Barnes' PII.

160. On September 2, 2022, Plaintiff Barnes received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Barnes suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Barnes suffered fraud in the form of unauthorized charges and an attempted theft of $1,000 worth of bitcoin and $329 of cash from her Paypal account. As a result of this fraud, Plaintiff Barnes spent time reviewing her accounts, disputing charges, and changing passwords.

161. Since learning about the Data Breach, Plaintiff Barnes has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and

obtaining and/or reviewing credit monitoring services through Credit Karma and Experian. To date, Plaintiff Barnes has spent 15-20 hours remediating the attempted fraud, as well as approximately 2 hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Barnes will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Barnes values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Barnes been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Barnes would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Barnes relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Barnes has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Barnes anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

LaShanna Beasley

162. Plaintiff LaShanna Beasley is, and was at all relevant times, a citizen and resident of the state of Tennessee. Starting in or around 2017 and continuing to 2022, Plaintiff Beasley has purchased a number of Samsung products including a Samsung television, Galaxy Active Watch, Galaxy S22 Ultra, Galaxy S21, and an S4 Watch. In connection with these purchases, Samsung gathered Plaintiff Beasley's PII.

163. On September 2, 2022, Plaintiff Beasley received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After

July 2022, Plaintiff Beasley suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Beasley suffered identity theft and fraud when an unauthorized North Carolina address appeared several times on her credit report. As a result of the fraud, Plaintiff Beasley has spent time disputing the address to the reporting agencies and monitoring her accounts.

164. Since learning about the Data Breach, Plaintiff Beasley has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Experian Identity and Credit Karma. To date, Plaintiff Beasley has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Beasley will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Beasley values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Beasley been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Beasley would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung Plaintiff Beasley relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Beasley has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Beasley anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Lorinda Hale

165. Plaintiff Lorinda Hale is, and was at all relevant times, a citizen and resident of the state of Tennessee. Since 2018 and continuing to 2022, Plaintiff Hale has purchased a number of Samsung products including a Galaxy S10, Galaxy S22, Galaxy Watch, and tablet. In connection with these purchases, Samsung gathered Plaintiff Hale's PII.

166. On September 2, 2022, Plaintiff Hale received a data breach notification letter from Samsung by email, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Hale suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Hale suffered fraud in the form of several unauthorized charges on her checking account in October or November 2022 and again in January 2023. As a result of this fraud, Plaintiff Hale spent time disputing the charges, and reviewing and monitoring her accounts.

167. Since learning about the Data Breach, Plaintiff Hale has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Experian and Capital One. To date, Plaintiff Hale has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Hale will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Hale values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Hale been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Hale would not have purchased the Samsung products or services or would have paid less

for them and would have limited the PII provided to Samsung. Plaintiff Hale relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Hale has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Hale anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

TEXAS

Aisha Suleiman

168. Plaintiff Aisha Suleiman is, and was at all relevant times, a citizen and resident of the state of Texas. Over the course of several years, Plaintiff Suleiman has purchased numerous Samsung products including smartphones, a Smart TV, Smart watches, and tablets. In or about May 2021, Plaintiff Suleiman purchased a Note 20. In connection with these purchases, Samsung gathered Plaintiff Suleiman's PII.

169. On September 2, 2022, Plaintiff Suleiman received a data breach notification letter from Samsung by text, notifying her that her PII was compromised in the Data Breach. After July 2022, Plaintiff Suleiman suffered injury and was damaged as a result of Samsung's failure to keep her PII secure. As a result of the Data Breach, Plaintiff Suleiman suffered misuse of her PII including a perceptible increase in scam/phishing emails, text messages, and phone calls. As a result of this misuse, Plaintiff Suleiman spent time fielding scam/phishing communications, conducting internet research and calling various agencies to get more information about how her information is being misused.

170. Since learning about the Data Breach, Plaintiff Suleiman has taken precautions to

mitigate the risk of future identity theft and fraud, including frequently checking her bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Experian. To date, Plaintiff Suleiman has spent several hours per week checking her credit and financial accounts for any unauthorized activity, a practice that Plaintiff Suleiman will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Suleiman values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Suleiman been informed that Samsung had insufficient data security measures to protect her PII, she would have taken this into account in making her purchasing decisions. Additionally, Plaintiff Suleiman would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Suleiman relied on Samsung's policies and promises to implement sufficient measures to protect her PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Suleiman has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Suleiman anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

WASHINGTON

Pratikkumar Patel

171. Plaintiff Pratikkumar Patel is, and was at all relevant times, a citizen and resident of the state of Washington. Before July 2022, Plaintiff Patel purchased a Samsung smartphone. In connection with that purchase, Samsung gathered Plaintiff Patel's PII.

172. On September 2, 2022, Plaintiff Patel received a data breach notification letter from

Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Patel suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Patel suffered a perceptible increase in scam/phishing emails, text messages, and phone calls.

173. Since learning about the Data Breach, Plaintiff Patel has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Experian. To date, Plaintiff Patel has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Patel will need to continue indefinitely to protect against fraud and identity theft. Plaintiff Patel values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Patel been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Patel would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Patel relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Patel has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Patel anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

Oliver Plummer

174. Plaintiff Oliver Plummer is, and was at all relevant times, a citizen and resident of

the state of Washington. Since 2005, Plaintiff Plummer purchased numerous Samsung products, including a Samsung washer/dryer, multiple Samsung televisions, Galaxy S21 and S22, and Samsung tablets. In connection with these purchases, Samsung gathered Plaintiff Plummer's PII.

175. On or about September 2, 2022, Plaintiff Plummer received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Plummer suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Plummer suffered fraud in the form of several unauthorized transactions, compromised social media accounts, and a fraudulent loan. As a result of this fraud, Plaintiff Plummer spent time disputing the charges, cancelling accounts and changing passwords.

176. Since learning about the Data Breach, Plaintiff Plummer has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; and obtaining and reviewing credit bureau reports. To date, Plaintiff Plummer has spent several hours per week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Plummer will need to continue indefinitely to protect against fraud and identity theft. To date, Plaintiff Plummer has spent several hundred dollars in remediation efforts to protect himself from harm resulting from the Data Breach. Plaintiff Plummer values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Plummer been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Plummer would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Plummer relied on Samsung's policies and

promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Plummer has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Plummer anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

WISCONSIN

Steven Baker

177. Plaintiff Steven Baker is, and was at all relevant times, a citizen and resident of the state of Wisconsin. Plaintiff Baker purchased a Samsung Galaxy Note 20 5G in approximately July 2022. In connection with that purchase, Samsung gathered Plaintiff Baker's PII.

178. On September 2, 2022, Plaintiff Baker received a data breach notification letter from Samsung by email, notifying him that his PII was compromised in the Data Breach. After July 2022, Plaintiff Baker suffered injury and was damaged as a result of Samsung's failure to keep his PII secure. As a result of the Data Breach, Plaintiff Baker suffered fraud in the form of an unauthorized bank charge on his debit card that was not reimbursed, as well as increased scam/phishing emails and text messages. As a result of this fraud, Plaintiff Baker spent time disputing the charge, reviewing and monitoring his accounts and changing his passwords.

179. Since learning about the Data Breach, Plaintiff Baker has taken precautions to mitigate the risk of future identity theft and fraud, including frequently checking his bank and credit card statements for unauthorized activity; obtaining and reviewing credit bureau reports; and obtaining and/or continuing credit monitoring services through Fisco and the credit reporting agencies. To date, Plaintiff Baker has spent approximately 5 hours a week checking his credit and financial accounts for any unauthorized activity, a practice that Plaintiff Baker will need to

continue indefinitely to protect against fraud and identity theft. Plaintiff Baker values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. Had Plaintiff Baker been informed that Samsung had insufficient data security measures to protect his PII, he would have taken this into account in making his purchasing decisions. Additionally, Plaintiff Baker would not have purchased the Samsung products or services or would have paid less for them and would have limited the PII provided to Samsung. Plaintiff Baker relied on Samsung's policies and promises to implement sufficient measures to protect his PII and privacy rights. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Baker has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Baker anticipates spending considerable time and money on an ongoing basis to mitigate and address the harms caused by the Data Breach.

B. Defendant

180. Defendant Samsung Electronics America, Inc. ("Samsung") is an active New York corporation with its headquarters and principal place of business located at 85 Challenger Road, Ridgefield Park, New Jersey 07660-2118.

181. Samsung is responsible for the production and sale of billions of dollars of Samsung consumer electronics sold in the United States, including: mobile telephones, tablets, smartwatches, and earbuds; TV & audio equipment; appliances, including refrigerators, ranges, dishwashers, microwaves, wall ovens, cooktops, range hoods, washers, dryers, steam closets, and vacuums; computers, monitors, and memory and storage devices; displays and digital signage; accessories for mobile devices, TV, audio, and appliance products; home security camera and surveillance systems; digital cameras; printers; and many more. Many of these products connect

to the internet ("Samsung Products").

182. Samsung also offers a wide variety of "Samsung Services," including SmartThings, which electronically connects a consumer's Samsung products; applications such as Samsung Health and Samsung Pay; and many other online and internet-connected services associated with Samsung devices (from mobile phones and tablets to TVs to home appliances and more).

183. Samsung maintains offices and employees who specifically oversee and handle data privacy and data policies and make data-driven decisions. The Samsung "Privacy Office" is located at 85 Challenger Road, Ridgefield Park, NJ 07660. *See* https://account.samsung.com/membership/terms/privacypolicy.

FACTUAL BACKGROUND

A. Samsung's Extensive Collection of Customers' PII for Samsung Accounts

184. Samsung collects and processes an enormous volume of the personal data of millions of consumers, including personal information obtained across all of Samsung's Internet-connected Products and Services, from mobile phones and tablets to TVs, home appliances, online services, and more.

185. Samsung strongly urges—or even requires—customers to create a "Samsung Account" upon purchasing or using its devices, appliances, and services. To create an account, customers must entrust Samsung with their PII, and creating an account authorizes Samsung to automatically collect significant additional data about the customer. Samsung explicitly warns customers that if they do not create a Samsung Account, do not provide all of the information Samsung requests, or instruct Samsung not to collect certain information about them, they may not be able to fully use the Products or Services that Samsung promotes. For example, the Samsung Pay U.S. Privacy Notice last revised on August 18, 2021 states: "Please note that if you decline to

allow Samsung Pay to collect, store or share certain information, you may not be able to use all of the features available through Samsung Pay."[3] The Samsung Privacy Policy for the U.S., updated on December 30, 2022, contains an almost identical warning: "If you decline to allow the Services to collect, store, or share certain information, you may not be able to enjoy full use of all of the features available through the Services."[4] Samsung explicitly states that a "Samsung Account" is the "gateway to the World of Samsung"[5] and "[h]aving a Samsung account is an essential part of owning a Samsung device. It lets you connect to the Samsung ecosystem and all of Samsung's related services."[6]

186. A Samsung Account allows customers to not only access certain features that improve the usability of the device, but also provides device-related benefits that only customers with a Samsung Account can access. Those benefits include, but are not limited to, backing up and syncing data, finding a device when it is lost, device support, coupons and discounts, and order tracking. Regardless of whether customers buy a printer, television, or a smartphone, they need to register their products with Samsung to access important features of their devices.

187. Consumers who purchase Samsung products are therefore essentially forced to register accounts; otherwise, many product features are locked/inaccessible, or it is nearly impossible to use the Products and Services in the way they were intended. For example,

---

[3] Samsung Pay U.S. Privacy Notice, Aug. 18, 2021, at 4, available at https://image-us.samsung.com/SamsungUS/home/support/samsung_pay/Samsung_Pay_Privacy_Notice.pdf (last accessed May 19, 2023).

[4] Samsung Privacy Policy for the U.S., Dec. 20, 2022, at 7, available at https://www.samsung.com/us/account/privacy-policy/ (last accessed May 19, 2023).

[5] SAMSUNG Account, Sign in to your Samsung account, available at https://account.samsung.com/accounts (last accessed May 19, 2023).

[6] *How to register a Samsung product with your Samsung account*, available at https://www.samsung.com/us/support/answer/ANS00089142/ (last accessed May 19, 2023).

consumers who purchase "smart" televisions typically do so because they want to watch streaming applications, such as Netflix or Hulu, on their televisions. To access those streaming applications, consumers download those applications and install them on their televisions. To download those applications, however, the Samsung smart television owner must first create a Samsung Account.

188. When a customer purchases a Samsung Product, creates a Samsung Account, or registers for or uses a Samsung Service, the customer may provide Samsung with PII such as:

- name;
- email address;
- postal address;
- phone number;
- payment card information (including name, card number, expiration date, and security code);
- date of birth;
- demographic data, *e.g.*, gender and age range;
- information stored in or associated with the customer's Samsung Account, including the customer's Samsung Account profile, ID, username, and password;
- username and password for participating third-party devices, apps, features, or services;
- information a customer stores on a Samsung device, such as photos, contacts, text logs, touch interactions, settings, and calendar information;
- recordings of a customer's voice when they use voice commands to control a service or contact Samsung's Customer Service team;
- transcripts of chat sessions, text messages, emails, and other communications when

the customer communicates with Samsung using these methods;

- information about products and services that customers purchase, obtain, or consider; and
- location data, including (1) the precise geolocation of a customer's device if the customer consents to the collection of this data; and (2) information about nearby Wi-Fi access points and cell towers that may be transmitted to Samsung when the customer uses certain Services.[7]

189. In addition to information the customer inputs for the Samsung Account, Samsung automatically collects even more information about the customer through means of browser cookies, pixels, web server logs, web beacons and other technologies when the customer uses Samsung "Services," which Samsung defines broadly as "all of [Samsung's] Internet-connected Samsung devices and services (from mobile phones and tablets to TVs, home appliances, online services, and more)," including:

a. data related to the customer's device, including MAC address, IP address, log information, device model, hardware model, the International Mobile Equipment Identity (IMEI) number, serial number, subscription information, device settings, connections to other devices, mobile network operator, web browser characteristics, application usage information, sales code, access code, current software version, Mobile Network Codes (MNC), subscription information, and randomized, non-persistent and resettable device identifiers, such as Personalized Service ID (PSID), and advertising IDs, including Google Ad ID;

b. data related to the customer's use of the Samsung Services, including

[7] Samsung, *Samsung Privacy Policy for the U.S.* (Dec. 30, 2022), available at https://www.samsung.com/us/account/privacy-policy/ (last accessed May 19, 2023).

clickstream data, the customer's interactions with the Services (such as the web pages visited, search terms, and the applications, services and features that are used, downloaded or purchased), the pages that lead or refer the customer to the Services, how the customer used the Services, and the dates and times of use of the Services; and

c. data related to the customer's use of third-party websites, applications and features that are connected to certain Samsung Services.[8]

190. Samsung collects information about what customers watch on its smart TVs, including which channels and programs the customers have watched. Samsung also "may obtain other behavioral and demographic data from trusted third-party data sources."[9]

191. Samsung collects extensive personal health information through its Samsung Health app, such as person's body composition and sleep patterns, as well as the kinds of exercise a person does and routes they follow when running or walking. It collects social security numbers, driver's license numbers, and other information when customers finance purchases of Samsung products through Samsung.

192. Samsung uses the information that it obtains directly from customers and that it collects automatically to, among other things:

a. "provide and enhance our Services, ***such as registering you or your device for a Service***, identifying and authenticating you so that you may use and interact with our Services (such as your device) and third-party services, and improving and customizing your experience within the Services" (emphasis added);

---

[8] Samsung, *Samsung Privacy Policy for the U.S.* (Dec. 30, 2022), available at https://www.samsung.com/us/account/privacy-policy/ (last accessed May 19, 2023).

[9] Zack Whittaker, *Parsing Samsung's Data Breach Notice*, TECHCRUNCH (Sept. 6, 2022), available at https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/ (last accessed May 19, 2023).

b. "operate, evaluate, and improve our business, including developing new products and services, managing our communications, analyzing our Services and customer base, conducting market research, aggregating and anonymizing data, performing data analytics, and undertaking accounting, auditing, and other internal functions;"

c. communicate with its customers;

d. support Samsung marketing activities and sales initiatives; and

e. "provide ads, which may include targeted (or interest-based) ads delivered on your Samsung device or within certain Samsung-branded apps."[10]

193. Of particular importance is Samsung's collection of geolocation data, including information sufficient to determine a person's street address and city ("precise geolocation data"), as well as their daily routines and associations, which can be used by bad actors (such as burglars and stalkers) to maliciously target individuals and their families.[11] Samsung ostensibly does not collect precise geolocation data without customer consent.[12] However, customers must give "consent" if they want to use many of the applications, features, and services associated with electronic devices: maps, directions, internet searches, ride-haling services, finding one's device or that of a child or other family member, tracking exercise activity, and so on. Samsung does not require "informed consent" for collection of precise geolocation data. For example, a user who turns "location" off may receive a message informing her that "[d]evice location for all

[10] Samsung, *Samsung Privacy Policy for the U.S.* (Dec. 30, 2022), available at https://www.samsung.com/us/account/privacy-policy/ (last accessed May 19, 2023).

[11] *FTC Testifies on Geolocation Privacy* (Jun. 4, 2014), available at https://www.ftc.gov/news-events/news/press-releases/2014/06.ftc-testifies-geoglocation-privacy (last accessed May 19, 2023).

[12] Samsung Account U.S. Privacy Notice Effective February 9, 2023 ("With your separate consent, we may use your precise geolocation…"; Samsung Ads Privacy Notice Effective January 1, 2020 ("Samsung gathers the following: . . . with your consent, precise geolocation data").

applications is turned off, and you may not be able to locate your device if it's lost" followed by two options: "Close" or "Turn on location."

194. The PII that Samsung collects from its customers is valuable to Samsung. Indeed, Samsung acknowledges this information "plays a key role in elevating what we do for our community" and that it "engage[s] with [Personally Identifiable Information] to inform and enhance everything from your experience to our communication, and to create and innovate radical solutions that help you overcome barriers."[13]

B. Samsung's Promises of Data Security and Privacy

195. Samsung is well aware that its customers value their own PII and that exposure of such PII presents a significant privacy risk. Samsung acknowledges that its customers "own" their "personal data" and recognizes the importance customers place on the value of their privacy.[14] Samsung's website states: "You own your privacy. We protect it."[15]

196. Because PII is valuable to Samsung's customers, and it can be maliciously used by unauthorized third parties, Samsung has made multiple promises about protecting it, including in the Samsung Privacy Policy for the U.S. (Dec. 30, 2022); Samsung Account Privacy Notice, Samsung Account U.S. Privacy Notice (Feb. 9, 2023); California Consumer Privacy Statement (Feb. 23, 2023); U.S. Consumer Privacy Rights, Policy & Security Principles (undated); Samsung Privacy Frequently Asked Questions; Samsung Our Approach to Privacy (undated); Welcome to Samsung Mobile Security (undated); Samsung Ads Privacy Notice (Jan. 1, 2020); Samsung Pay

[13] *Samsung's Privacy Principles*, available at https://www.samsung.com/us/privacy/ (last accessed May 19, 2023).

[14] Samsung Privacy, *Frequently Asked Questions (FAQ)*, available at https://sdapla.privacy.samsung.com/privacy/br/anonymous/faq.do (last accessed May 19, 2023).

[15] *Samsung's Privacy Principles*, available at https://www.samsung.com/us/privacy/ (last accessed May 19, 2023).

Privacy Notice (Aug. 18, 2021); Samsung Local Privacy Policy SmartTV Supplement (undated); Samsung Display Solutions Privacy Policy (Mar. 30, 2021); and Samsung Privacy (undated).

197. The abundant Samsung privacy promises include:

- "[W]e prioritize protecting your information;"
- "We take data security very seriously. Our products are designed to keep your data private and secure …;"[16]
- Samsung devices and services are "designed with privacy and security at top of mind;"[17]
- "We are committed to protecting your privacy …;"[18]
- "At Samsung Mobile, security and privacy are at the core of what we do and what we think about every day;"[19]
- Samsung has "industry-leading security;"[20] and
- Samsung takes "a holistic approach to security to ensure that, at all levels of the device, we are protecting users' security and privacy at all times."[21]

198. In addition to complying with its promises and assurances to its customers,

[16] *Samsung's Privacy Principles*, available at https://www.samsung.com/us/privacy/ (last accessed May 19, 2023)

[17] Samsung, *Our Approach to Privacy*, available at https://www.samsung.com/us/account/our-approach-to-privacy/ (last accessed May 19, 2023)

[18] *Id.*

[19] Samsung, *Welcome to Samsung Mobile Security*, available at https://security.samsungmobile.com/main.smsb (last accessed May 19, 2023)).

[20] *Id.*

[21] Samsung, *Welcome to Samsung Mobile Security*, available at https://security.samsungmobile.com/main.smsb (last accessed May 19, 2023).

Samsung must comply with security guidelines and recommendations the Federal Trade Commission ("FTC") has promulgated to reduce the likelihood of data breaches like that which occurred at Samsung.[22] Among the FTC's recommendations are: limiting the sensitive consumer information a business keeps; encrypting sensitive information sent to third parties or stored on computer networks; and identifying and understanding the company's network vulnerabilities. The occurrence of the Data Breach and Samsung's failure or inability to provide victims with more specific information about the amount and kind of compromised PII illustrate Samsung's failure to deliver on its promises and obligations.

199. Plaintiffs and other Class Members relied to their detriment on Samsung's numerous false representations regarding data security. In addition, Samsung misled them by not disclosing or warning about its inadequate security protections, or that Samsung would forever store customers' PII without properly protecting it, or the foreseeable and likely data breach that would result from its failure to properly protect the PII it collected.

200. Had Samsung disclosed to Plaintiffs and Class Members that its data systems were not secure and were vulnerable to attack, Plaintiffs would not have bought certain Samsung products and services or would have paid less for them; would not have used the Samsung Services and Samsung Products that led to the account creation; and/or would have provided less information to Samsung. Thus, Plaintiffs and Class Members significantly overpaid Samsung based on what the products were represented to be worth compared to what they actually were worth.

[22] Federal Trade Commission, Data Security, available at https://www.ftc.gov/business-guidance/privacy-security/data-security (last accessed May 19, 2023); Federal Trade Commission, Business Guidance, available at https://www.ftc.gov/business-guidance (last accessed May 19, 2023).

201. Samsung has obligations created by contract, industry standards, common law, and its own privacy policies and representations to its customers to keep PII confidential and protect it from unauthorized disclosures like that which occurred in the Data Breach.

202. Samsung enriched itself by collecting and using a treasure trove of sensitive PII from Plaintiffs and Class Members for its own benefit. Yet it failed to spend enough of the money it made from that valuable information to employ reasonable, accepted safety measures to secure the information.

C. Samsung's Recent History of Data Breaches

203. Samsung is no stranger to data security incidents, as its lax security practices have resulted in multiple disclosures of customers' sensitive personal information, including the data breach at issue in this case. Since 2019, Samsung has experienced a number of data security incidents and data breaches that have allowed hackers to access the sensitive data of Samsung customers and Samsung's internal company data.

204. In May 2019, a security researcher with cybersecurity firm, SpiderSilk, discovered that dozens of Samsung internal coding projects were being exposed on GitLab, an open-source code repository and collaborative software development platform, because they were erroneously configured as public without any password protection.[23]

205. As a result, anyone could access Samsung internal coding projects and download the source code, including source code for the Samsung smart home ecosystem platform known as SmartThings, its Bixby digital assistant, and private certificates for both the Android and iOS

[23] Davey Winder, *Samsung Investigates Massive Data Leak -- What You Need To Know*, FORBES, (May 9, 2019), available at https://www.forbes.com/sites/daveywinder/2019/05/09/samsung-investigates-massive-data-leak-what-you-need-to-know/?sh=1622b10b2e2c (last accessed May 19, 2023).

SmartThings applications. The researcher had the private token of a user with full access to 135 projects on GitLab. These were the "keys to the Samsung code kingdom" that the researcher could have used to access the account of that staff member. A malicious actor could have injected malicious code into a major Samsung application.[24]

206. In February 2020, a glitch in certain Samsung smartphones briefly gave users of these phones the ability to access information belonging to other users, "including names, addresses and the last four digits of their payment cards."[25]

207. Furthermore, in 2020, researchers discovered that Samsung smartphones sold "from late 2014 onward" suffered from a "critical security vulnerability" that allowed hackers to penetrate and install malicious code on Samsung smartphones without any interaction from the phone's owner. Although the vulnerability was eventually mitigated by a software update, this issue—described as being "about as dangerous as things can be"—underscores Samsung's history of inadequate security practices. The vulnerability affected every Galaxy smartphone that Samsung had made from late 2014 until February 2020.[26]

208. In or around April 2022, an organization called Lapsus$ accessed and stole 190GBs of confidential Samsung data, including a host of confidential and valuable technical data.[27]

---

[24] *Id.*

[25] Harry Domanski, *Samsung admits to leaking personal data of around 150 users*, TECHRADARPRO (Feb. 24, 2020), available at https://www.techradar.com/news/samsung-admits-to-leaking-personal-data-of-around-150-users (last accessed May 19, 2023).

[26] Davey Winder, *Samsung Confirms Critical Security Issue for Millions: Every Galaxy After 2014 Affected*, FORBES, (May 7, 2020) available at https://www.forbes.com/sites/daveywinder/2020/05/07/samsung-confirms-critical-security-warning-for-millions-every-galaxy-after--2014-affected/?sh=1f24dcad3af7 (last accessed May 19, 2023).

[27] *See* Mike Moore, *Samsung Confirms Data Breach, Personal Customer Data Stolen*, TECHRADARPRO (Sept. 5, 2022), available at https://www.techradar.com/news/samsung-confirms-data-breach-personal-customer-data-stolen (last accessed May 19, 2023).

Lapsus$ claimed to have taken the sources for every Trusted Applet installed in Samsung's TrustZone environment used for sensitive operations; algorithms for all biometric unlock operations; bootloader source code for all recent Samsung devices; confidential source code from Qualcomm; source code for Samsung's activation servers; and full source code for technology used for authorizing and authenticating Samsung accounts, including APIs and services. Lapsus$ later published 190GB of Samsung's confidential data online.

209. Despite the earlier data security incidents, full knowledge that sensitive technical data had been exposed months before, and the immediate need to protect customers' private information and data from Lapsus$ and the other attackers, Samsung did not promptly detect the Data Breach, did not promptly disclose the Data Breach after discovering it, and tried to downplay the injury caused by the Data Breach (while simultaneously warning consumers not to click on links or attachments in unexpected or suspicious emails and to take care when dealing with any communications asking for their personal information).[28]

210. Samsung's cavalier stance regarding data security is highly likely to lead to more security incidents that further compromise Plaintiffs' and Class Members' PII. Indeed, Samsung's string of data breaches has continued since the Data Breach at issue in this action. Just this January, a "pro-Russian hacktivist group" called "Genesis Day" breached Samsung's systems and retrieved sensitive corporate information including "employee access credentials," certain internal instructional videos, "and the necessary procedures for Samsung's internal system login."[29] And

[28] *See* Important Notice Regarding Customer Information, SAMSUNG (September 2, 2022), available at https://www.samsung.com/us/support/securityresponsecenter/ (last accessed on May 19, 2023).

[29] *See* Vilius Petkauskas, *Pro-Russian hackers say they breached Samsung*, CYBERNEWS (Jan. 18, 2023), https://www.cybernews.com/cyber-war/russian-hackers-claim-samsung-breach/ (last accessed May 19, 2023).

in December 2022, professional hackers demonstrated the vulnerability of Samsung's systems by hacking into the Samsung Galaxy S22 twice during a hacking competition.[30]

D. The Data Breach and Samsung's Delayed Disclosure

211. On September 2, 2022, the Friday before Labor Day, when much of the U.S. was already focused on the holiday weekend, Samsung finally disclosed the Data Breach. Samsung posted a public announcement on its website https://www.samsung.com/us/support/securityresponsecenter/, but its primary method of notifying customers that their PII had been compromised in a data breach (the "Notice") was through email. Because mass email messages often go directly to junk or spam folders or look innocuous or unimportant enough to be deleted without being read, it is likely that many of the persons affected by the Data Breach did not receive the Notification. Those who did receive it did not receive very detailed information; the vague statement announced that Samsung's "U.S. systems" had been infiltrated "[i]n late July 2022" by "an unauthorized third party" that then stole PII that Plaintiffs and Class Members had entrusted to Samsung.

212. Despite being one of the world's largest technology companies, Samsung claims that it did not discover the breach until weeks after the fact, on August 4, 2022. By then, the fraudsters could have accessed and misused significant amounts of PII belonging to Plaintiffs and Class Members. Samsung then compounded the damage inherent in its belated discovery of the breach by waiting nearly an additional month to disclose the Data Breach to affected customers and the public at large.

[30] *See* Davey Winder, *Zero-Day Hackers Breach Samsung Galaxy S22 Twice in 24 Hours*, FORBES (Dec. 7, 2022), available at https://www.forbes.com/sites/daveywinder/2022/12/07/zero-day-hackers-breach-samsung-galaxy-s22-twice-in-24-hours/?sh=5ca8fd5f76ac (last accessed May 19, 2023).

213. Not only was the disclosure inexcusably late, it also was unconscionably vague and self-serving. Instead of providing detailed information that customers could use to protect themselves, the announcement on Samsung's website merely stated that the data breach may have affected customers' PII such as name, contact and demographic information, date of birth, and product registration information. To add further confusion, Samsung also claimed that "[t]he information affected for each relevant customer may vary."

214. Samsung's carefully worded statement failed to shed light on many of the details surrounding the Data Breach. It did not address crucial aspects such as the origin of the breach; how it was uncovered; the scope of Samsung systems affected; the reasons for the nearly month-long delay in disclosing the Data Breach; the number of Samsung customers impacted; the duration of the investigation; the extent of customer data accessed, including the number of years and volume; the nature of demographic data stolen; the precise extent of the PII compromised; or whether this Data Breach was connected to an earlier one involving Samsung's internal data.

215. The announcement did not even disclose how many customers' PII was breached. Upon information and belief, more than half of Samsung's U.S. consumers had their PII compromised in the breach. A technology journalist noted that what Samsung "leaves out" of its poorly explained data breach notice is more important than what it disclosed about the breach. Samsung's public relations firm declined to answer questions from the journalist.

216. When Samsung wrote that data was "acquired," it meant that hackers exfiltrated the data. If hackers stole data, the network was not set up properly, Samsung did not protect that data, and the hackers deeply penetrated Samsung's network. Further, Samsung's statement that "in some cases" the hackers took customer names, contact and demographic information, date of birth and product registration," suggests Samsung was trying to limit what it shared with the public about

the breach or that it did not investigate the extent of the PII stolen during the Data Breach as quickly and as well as it should have.[31]

217. Because Samsung "did not specify which type of customers—business or consumer, for example—were impacted, give a breakdown of affected regions or provide any other information . . . all customers [should] conclude that their data is part of the breach."[32]

218. The notifications that Samsung emailed directly to consumers beginning around September 2, 2022, were no better than its public disclosure. Plaintiffs and potential Class Members received emails stating that Samsung had "recently discovered a cybersecurity incident" that affected some of their personally identifiable information.

219. The notice of the Data Breach emailed to Plaintiffs was sent from the email address samsung@innovations.samsungusa.com by Samsung Electronics America, Inc., 85 Challenger Road, Ridgefield Park, NJ 07660.

220. Samsung's email notification to Plaintiffs and Class Members merely regurgitated the same vague information stated in the website announcement. The Notification stated that "[i]n late July 2022, an unauthorized third party acquired information from some of Samsung's U.S. systems" and on or around August 4, 2022, Samsung determined that "personal information of certain customers was affected." Samsung determined the affected information included "name, contact and demographic information, date of birth and product registration information" and the information affected could vary for each relevant customer.

---

[31] *See* Zack Whittaker, *Parsing Samsung's Data Breach Notice*, TECHCRUNCH (Sept. 6, 2022), available at https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/ (last accessed May 19, 2023).

[32] Allen Bernard, *Impact of Samsung's Most Recent Data Breach Unknown*, TECH REPUBLIC (Sept. 9, 2022), available at http://www.techrepublic.com/article/samsung-data-breach/ (last accessed May 19, 2023).

221. Furthermore, the timing of Samsung's announcement and Notice functioned to minimize consumer awareness. Chris Clements, Vice President of Solutions Architecture at Cerberus Sentinel, a provider of cybersecurity and compliance services, noted that Samsung's "lack of transparency on the number of individuals impacted as well as the delay in notifying them combined with a late Friday holiday weekend release seem like clear attempts to minimize the incident."[33]

222. Samsung's Notice also fell woefully short of the requirements imposed by certain state data security statutes, such as California Civil Code, Section 1798.82(d)(1), which required Samsung to title the notice "Notice of Data Breach," and to present specific information under the headers "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Samsung's Notice did not even attempt to comply with these formatting requirements, which are "designed to call attention to the nature and significance of the information" the notice contains. Cal. Civ. Code § 1798.82(d)(1). California law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General, but a search for "Samsung" on the applicable website results in a message that "[t]here are currently no published reported breaches."[34]

223. Samsung's failure to provide prompt and adequate notification of the Data Breach injured Plaintiffs and Class Members. Timely and complete notification of a data breach is essential so that consumers can take steps to prevent misuse of the information, mitigate harm that has already occurred, and avoid additional harm.

---

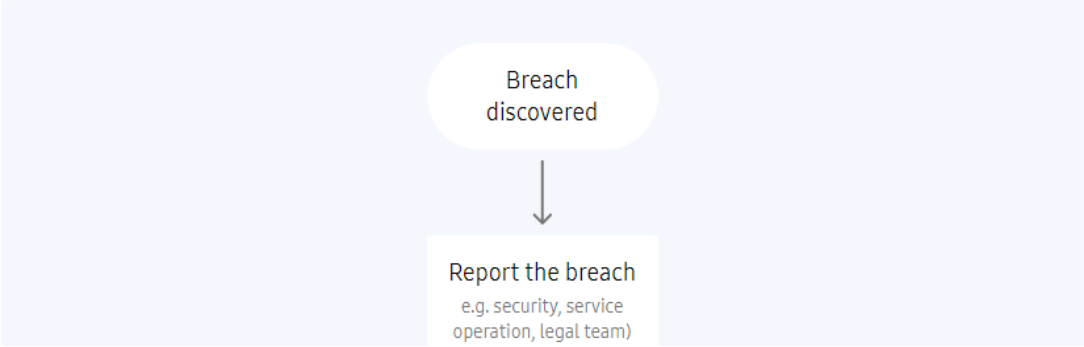
[33] Allen Bernard, *Impact of Samsung's Most Recent Data Breach Unknown*, TECHREPUBLIC (Sept. 9, 2022), available at http://www.techrepublic.com/article/samsung-data-breach/ (last accessed May 19, 2023).

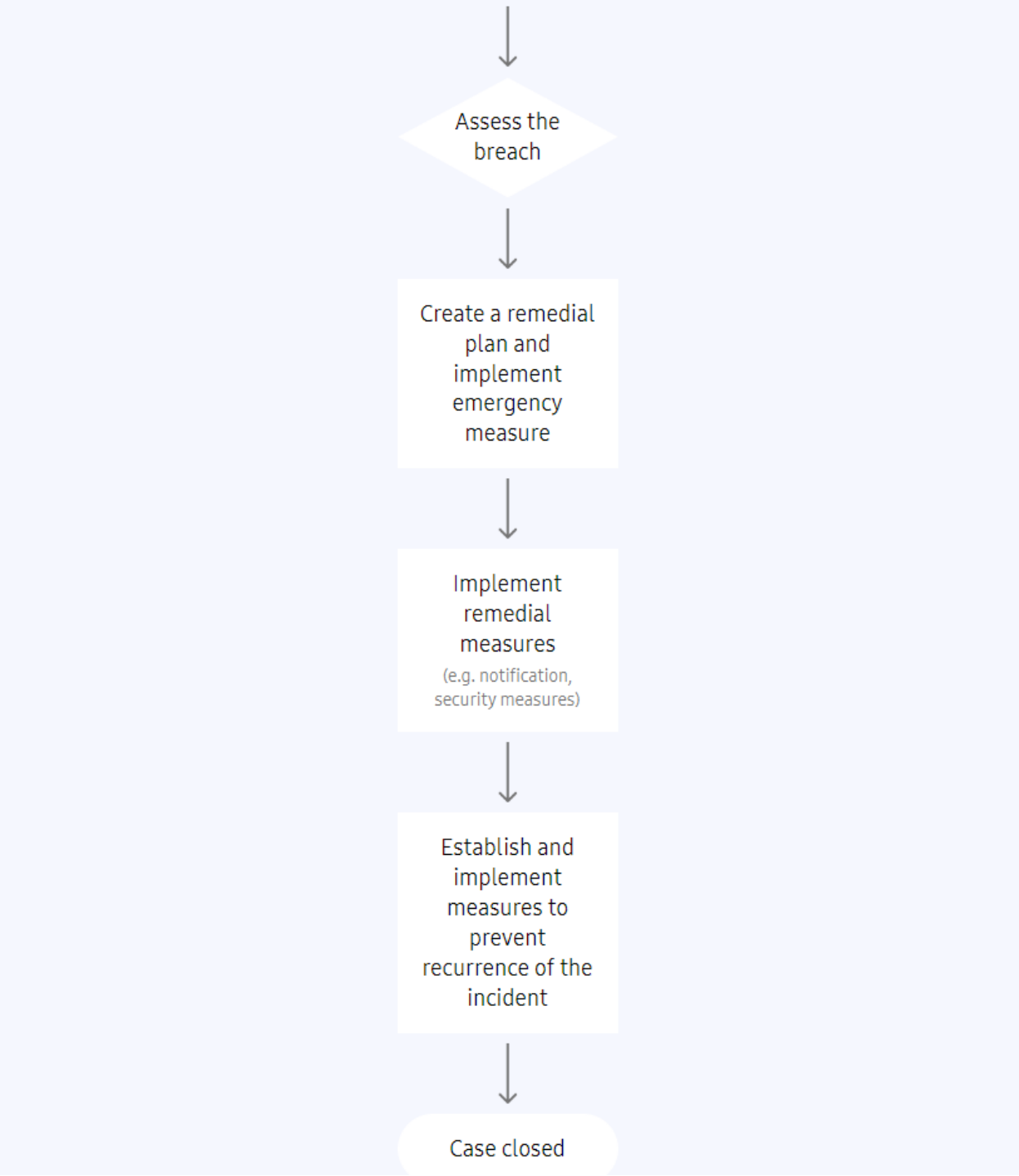
[34] State of California Department of Justice, *Search Data Security Breaches*, available at https://www.oag.ca.gov/privacy/databreach/list (last accessed May 19, 2023).

224. Samsung' response to the Data Breach did not even comply with the procedures it says it will follow "immediately upon detection of" a data breach incident:

At Samsung Electronics, we have a data breach response process in place that enables the company to assess a data breach incident and to take remedial measures immediately upon detection of the incident. We promptly notify and report to the affected users and the relevant authority respectively in compliance with the applicable data protection laws. Where a notification is provided to the affected users, the following information are communicated via e-mail, SMS, or a notice on our website, the category of the breached data, when and how the breach occurred, the measures that the affected users can take to minimize the damage, the remedial measures taken by us and our point of contact for any queries by the affected users. We take all and every action to prevent data breach incident and to minimize any damage to our users in the case of such an incident.

Procedure for Privacy Incident Response





https://www.samsung.com/global/sustainability/popup/popup_doc/AYUqnfrKC-4AIx_C/

225. When consumers are promptly notified of a data breach that may have included sensitive personal information, they can check for signs of identity theft, such as new accounts or

loans in their name. Consumers can also take protective measures such as changing passwords on affected accounts to prevent unauthorized access, placing a freeze on their credit reports to prevent criminals from opening new accounts or obtaining loans in their name, and monitoring financial accounts for suspicious activity, such as unauthorized transactions or changes to account information. After a data breach, consumers may receive phishing emails or calls from criminals posing as family, friends, or legitimate companies; timely notification can help consumers be more cautious and vigilant in their online and telephonic interactions. The later consumers receive notice, the less effective these measures may be.

226. The FTC recommends that businesses have a comprehensive communication plan that reaches all affected audiences—employees, customers, investors, business partners, and other stakeholders—in the case of a data breach. This plan should be designed to quickly notify people that their personal information has been compromised so that they can take steps to reduce the chance that their information will be misused.

227. The FTC also instructs businesses to provide detailed notices to affected parties that "clearly describe what you know about the compromise." This information, at a minimum, should include: "how it happened; what information was taken; how the thieves have used the information (if you know); what actions you have taken to remedy the situation; what actions you are taking to protect individuals, such as offering free credit monitoring services; and how to reach the relevant contacts in your organization."[35]

E. It is Likely that Criminals Exfiltrated Highly Sensitive Geolocation Data

228. Due to Samsung's wholly inadequate disclosures, consumers still do not have a

[35] Federal Trade Commission, *Data Breach Response: A Guide for Business,* at 6, available at https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed May 19, 2023).

clear understanding of what data was acquired by hackers. Samsung has not provided any additional detail beyond the extremely vague disclosure that "information such as name, contact and demographic information, date of birth, and product registration information" was "affected."[36]

229. Of great concern is Samsung's admission that "demographic information" was exfiltrated. The website TechCrunch examined Samsung's privacy policies and concluded that demographic information may include customers' "precise geolocation data," which can be used to identify where customers go and with whom they meet.[37]

230. Neither Samsung's U.S. Privacy Policy nor Samsung's Announcement nor the Notifications to customers about the Data Breach clearly defines the "demographic information" that was compromised. The Notification pointed to Samsung's Ads Privacy Policy as a potential source of clarification of its demographic information sharing policies.[38]

231. The Ads Privacy Policy that has been in effect since January 1, 2020, is hardly a model of clarity or specificity. It states that Samsung Ads service (the "Service") "provides Customized Ads by using unique, randomized, non-persistent, and resettable device identifiers, known as 'Advertising ID' on Samsung mobile devices and 'PSID' on Samsung Smart TVs." The Ads Privacy Policy further states:

The Service may deliver Customized Ads based on your demographic

[36] Important Notice Regarding Customer Information, SAMSUNG (September 2, 2022), available at https://www.samsung.com/us/support/securityresponsecenter (last accessed May 19, 2023).

[37] Zack Whittaker, *Parsing Samsung's Data Breach Notice*, TECHCRUNCH (Sept. 6, 2022), available at https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice (last accessed May 19, 2023).

[38] Important Notice Regarding Customer Information, SAMSUNG (September 2, 2022), available at https://www.samsung.com/us/support/securityresponsecenter (last accessed May 19, 2023).

characteristics, preferences, choices, and interests by obtaining the following information:

- device identifiers and device settings information (*e.g.*, device manufacturer, model, OS version, IP address, Advertising IDs, device connection status, mobile country code, mobile network code, language, and mobile carrier);

- device usage and log information (*e.g.*, list of installed apps, app version, and app usage statistics);

- information about your interactions with Customized Ads (*e.g.*, the ads you click on);

- if you are a Customization Service user who has opted in to receive Customized Ads, inferences drawn from the data collected by the Customization Service (*e.g.*, behaviors and preferences) and, with your consent, precise geolocation data; and

- if you are a Samsung Smart TV user who has opted into both Viewing Information Services and Interest-Based Advertising, TV viewership data (*e.g.*, information about the networks, channels and websites visited, programs viewed, and amount of time spent viewing Smart TV content).

p> [*sic*] We also may obtain other behavioral and demographic data from trusted third-party data sources. We may use this data to draw inferences about your preferences, choices, and interests to provide you with Customized Ads about products and services tailored to your individual interests. We may collect and combine information about your online activities over time and across Samsung and third-party devices, apps, websites and online services to provide you with Customized Ads.[39]

232. The Ads Privacy Policy states that customers may opt out of receiving Customized Ads but does not indicate that doing so stops Samsung from collecting the customer's "demographic characteristics" or any other data.

233. Although the Ads Policy states that Samsung collects precise geolocation data "only with consent," as described above (a) such consent is hardly "informed" consent, and (b)

[39] *Samsung Ads Privacy Notice* (Effective January 1, 2020), available at https://www.samsung.com/us/account/privacy-policy/samsungads/ (last accessed May 19, 2023).

customers must provide that consent to use many important features of Samsung's products.[40] Thus, in the absence of any indication to the contrary from Samsung, Plaintiffs and Class Members must assume that the "demographic data" compromised in the Data Breach includes precise geolocation data.

234. On the same day Samsung announced its data breach, Samsung also pushed out a new privacy policy to its users.[41] The Privacy Policy update changed the generic notice that demographic data was used for customized ads into a notice that Samsung may track Samsung users' physical location via their devices, either as part of a security feature or to serve specific advertising for nearby Samsung or third-party stores, with separate consent.[42]

F. Damages Resulting From Exfiltration of Geolocation Data

235. The exfiltration of geolocation data poses significant and grave concerns for Plaintiffs and Class Members.

236. The FTC categorizes geolocation data as sensitive personal information and has warned about the potential privacy risks associated with its collection and use.[43] Among other things, "geolocation information can reveal a consumer's movements in real time, as well as

[40] *Id.*

[41] *See* Zack Whittaker, *Parsing Samsung's Data Breach Notice*, TECHCRUNCH (Sept. 6, 2022), available at https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice (last accessed May 19, 2023).

[42] Samsung Account, *Privacy Notice, Samsung account U.S. Privacy Notice* (Effective Feb. 9, 2023), available at https://account.samsung.com/membership/policy/privacy (last accessed May 19, 2023).

[43] *FTC Testifies on Geolocation Privacy* (June 4, 2014), available at https://www.ftc.gov/news-events/news/press-releases/2014/06/ftc-testifies-geolocation-privacy (last accessed May 19, 2023).

provide a detailed, comprehensive record of a consumer's movements over time."[44]

237. Where geolocation data can be tied to a particular individual, the harms associated with the distribution of detailed geolocation data may outweigh countervailing benefits to consumers or competition. For example, precise geolocation data tied to an individual can invade the person's privacy, be used to maliciously track and target a person and his or her family, and subject that person to harassment or discrimination based on his or her perceived political beliefs, religious affiliation, sexual orientation, mental or physical health status, immigration status, or other personal characteristics.

238. The FTC and the U.S. Government Accountability Office ("GAO") have warned that geolocation data can be used to track individuals' movements and activities over time, making them vulnerable to crimes ranging from burglary and theft, to stalking, kidnapping, child abduction, and domestic violence.[45]

239. The FTC recognizes unauthorized tracking of individuals and selling aggregated geolocation data without proper protection against tying data to specific individuals as unfair trade

[44] Jessica Rich, *Prepared Statement of the Federal Trade Commission On S. 2171, The Location Privacy Protection Act of 2014,* Before the Subcommittee For Privacy, Technology and the Law of the Committee on the Judiciary, United States Senate (June 4, 2014), available at https://www.judiciary.senate.gov/imo/media/doc/06-04-14RichTestimony.pdf (last accessed May 19, 2023).

[45] Jessica Rich, *Prepared Statement of the Federal Trade Commission On S. 2171, The Location Privacy Protection Act of 2014,* Before the Subcommittee For Privacy, Technology and the Law of the Committee on the Judiciary, United States Senate (June 4, 2014), available at https://www.judiciary.senate.gov/imo/media/doc/06-04-14RichTestimony.pdf (last accessed Apr. 3, 2023); *Mobile Device Location Data, Additional Federal Actions Could Help Protect Consumer Privacy*, Report to the Chairman, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate, at 16-17 (Sep. 2012), available at https://www.gao.gov/assets/gao-12-903.pdf (last accessed May 19, 2023).

practices.[46]

240. The harms identified by the FTC apply to Plaintiffs and Class Members. Because of the indispensable nature of connected devices to the entire spectrum of daily life, many Americans carry their mobile devices everywhere they go. For instance, a 2015 study found that 94% of smartphone owners said they carry their phone with them frequently, and 82% say they never or rarely turn their phones off.[47]

241. Upon information and belief, geolocation data was exfiltrated in the Data Breach and sold or can be sold on the underground market, which has caused and will continue to cause Plaintiffs and the Class emotional distress and expose them to additional injury and a heighted personal safety risk.

G. Data Breaches Lead to Identity Theft

242. The exfiltration of PII in a data breach has serious consequences for consumers, including financial loss, reputational damage, and identity theft. Consumers whose PII is exfiltrated are at substantially higher risk of identity fraud, which has enormous consequences for those individuals and the United States economy as a whole. For example, in 2021, overall identity fraud damages suffered by U.S consumers reached $43 billion.[48]

---

[46] *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission* (June 22, 2016), available at https://www.ftc.gov/news-events/news/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked-hundreds-millions-consumers (last accessed May 19, 2023); *Federal Trade Commission v. Kochava Inc.,* Case No. 2:22-cv-00377-DCN (D. Idaho).

[47] Lee Rainie and Kathryn Zickuhr, *Americans' Views on Mobile Etiquette*, Pew Research Center (Aug. 26, 2015), available at https://www.pewresearch.org/internet/2015/08/26/americans-views-on-mobile-etiquette/ (last accessed May 19, 2023).

[48] Javelin Strategy & Research, *Total Identity Fraud Losses Soar to $56 Billion in 2020* (Mar. 23, 2021), available at https://javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020 (last accessed May 19, 2023).

243. Once the PII was exfiltrated in a data breach, it became available for other persons to sell or trade. The exfiltrated PII will continue to be at risk for the indefinite future. This general problem is made more acute by the fact that Samsung did not notify consumers of the breach until almost two months after it occurred.

244. Samsung customers whose PII was compromised by the Data Breach are also more vulnerable to "SIM-swap" attacks. A SIM-swap attack occurs when scammers trick a telephone carrier into posting the victim's phone number to the scammer's SIM card. By doing so, the attacker can bypass two-factor authentication, which normally is an important means of protecting financial and other important accounts, including cryptocurrency wallets.

245. Moreover, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach.

H. Samsung Should Have Increased Data Security

246. In the years immediately preceding the Data Breach, Samsung knew or should have known that its computer systems were a target for cybersecurity attacks.

247. For example, in April 2020, ZDNET reported that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[49]

248. Thousands of similar articles, warnings, White Papers, studies, and reports on data

[49] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year* (Apr. 30, 2020), available at https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed May 19, 2023).

security for businesses have publicized the increasing threat of data breaches to companies of all sizes.

249. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Samsung on notice, long before the Data Breach, that (1) cybercriminals were targeting large, public companies such as Samsung; (2) cybercriminals were ferociously aggressive in their pursuit of large collections of PII like that in possession of Samsung; (3) cybercriminals were selling large volumes of PII and corporate information on Dark Web portals; and (4) the threats were increasing.

250. Had Samsung been diligent and responsible, it would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key ***avoidable*** causes for data security incidents are:

- Lack of a complete risk assessment, including internal, third-party, and cloud-based systems and services;
- Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;
- Misconfigured devices/servers;
- Unencrypted data and/or poor encryption key management and safeguarding;
- Use of end-of-life (and thereby unsupported) devices, operating systems, and applications;
- Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;
- Failure to block malicious email; and

- Users succumbing to business email compromise (BEC) and social exploits.[50]

251. Samsung knew, or should have known, that the PII of individuals is highly valuable to criminals, selling at $40 to $200 for names, addresses, credit histories, and phone numbers.[51] Experian publishes selling prices for individual items of PII and reported that stolen credit card or debit card numbers can sell for $5 to $10 apiece on the Dark Web.[52] TECHREPUBLIC reported in 2021 that the average price for PII in the U.S. was $8, but there could be a wide range of values for data packages with multiple pieces of data for each individual, such as that stolen from Samsung.[53]

252. In light of the information and warnings readily available to Samsung before the Data Breach, Samsung had reason to be on guard and to increase data security to avoid an attack.

253. Prior to the Data Breach, Samsung knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated and published as the result of a cyberattack.

---

[50] Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), available at https://www.proofpoint.com/us/security-awareness/post/ota-report-indicates-93-security-breaches-are-preventable (last accessed May 19, 2023).

[51] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed May 19, 2023).

[52] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN CYBERSECURITY (Dec. 6, 2017), available at https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 19, 2023).

[53] Jonathan Greig, *How much is your info worth on the Dark Web? For Americans, it's just $8,* TECHREPUBLIC (Feb. 8, 2021), available at https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-dark-web-for-americans-its-just-8/#:~:text=Personal%20information%20from%20US%20citizens,from%20tech%20research%20firm%20Comparitech. (last accessed May 19, 2023).

254. Prior to the Data Breach, Samsung knew or should have known that it should encrypt the sensitive data elements within the PII it collected so that it would be protected against publication and misuse in the event of a data breach.

255. Data security experts advise that "the vast majority of data breaches are preventable" if companies follow widely-available advice on data security practices, including "continually audit[ing] and reevaluat[ing]" their data security practices; being aware of and working proactively to counter cybercriminals' evolving techniques and approaches; and training and re-training their employees.[54] Upon information and belief, Samsung did not follow this advice.

CLASS ACTION ALLEGATIONS

NATIONWIDE CLASS

256. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs bring this case as a class action on behalf of the following nationwide class (the "Nationwide Class" or the "Class"):

> All persons residing in the United States whose Personally Identifiable Information was accessed, compromised, or stolen in the data breach announced by Samsung on September 2, 2022.

This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

257. The Nationwide Class asserts claims against Samsung for Negligence (Count 1), Negligence *Per Se* (Count 2), Breach of Confidence (Count 3), Breach of Express Contract (Count

[54] Nate Nead, *How To Prevent A Data Breach In Your Company*, FORBES BUSINESS COUNSEL, FORBES (Jul. 30, 2021) available at https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=3828f7b918da (last accessed May 19, 2023).

4), Breach of Implied Contract (Count 5), Unjust Enrichment (Count 6, pled in the alternative), and Declaratory Judgment (Count 7).

STATEWIDE SUBCLASSES

258. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs bring this case as a class action and bring pertinent statutory or common law claims on behalf of subclasses for residents of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Washington, Wisconsin (the "State Subclasses"). Each State Subclass is defined as follows:

> All persons residing in [name of jurisdiction] whose Personally Identifiable Information was accessed, compromised, or stolen in the data breach announced by Samsung on September 2, 2022.

This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

259. Excluded from the Nationwide Class and each Subclass are Samsung and Samsung's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Samsung has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

260. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

261. **Numerosity, Fed R. Civ. P. 23(a)(1).** The Nationwide Class and each of the State Subclasses (the "Classes") are so numerous that joinder of all members is impracticable. Samsung discovery will ultimately identify thousands of customers whose PII may have been improperly accessed in the Data Breach. Those individuals' names and addresses are available from Samsung's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Subclass, making joinder of all Subclass Members impracticable.

262. **Commonality and Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3).** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include, but are not limited to, the following:

a. Whether Samsung collected Plaintiffs' and Class Members' PII;

b. Whether Samsung represented to Plaintiffs and the Classes that Samsung would protect Plaintiffs' and Class Members' PII;

c. Whether Samsung owed a duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Samsung breached a duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Samsung has a contractual obligation to safeguard Plaintiffs' and Class Members' PII;

f. Whether Samsung's conduct breached any contractual obligation to protect Plaintiffs' and Class Members' PII;

g. Whether Samsung knew or should have known that its systems were

vulnerable to a data breach;

h. Whether Samsung was negligent in failing to implement proper security procedures and practices;

i. Whether Samsung's security measures to protect its systems were reasonable in light of known legal requirements;

j. Whether Samsung notified Plaintiffs and Class Members that their PII had been compromised as soon as practicable and without unreasonable delay after the data breach was discovered;

k. Whether the content of Samsung's notice to Plaintiffs and Class Members that their PII had been compromised was adequate in light of known legal requirements;

l. Whether Samsung violated its common law duties to Plaintiffs and Class Members by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

m. Whether Samsung properly addressed the vulnerabilities that permitted the Data Breach to occur;

n. Whether Samsung's conduct injured Plaintiffs and the Class;

o. Whether Samsung's conduct violated state consumer protection laws;

p. Whether Samsung's conduct violated state data privacy laws;

q. Whether Samsung's conduct violated state data breach laws;

r. Whether Plaintiffs and Class Members are entitled to actual damages and/or punitive damages as a result of Samsung's wrongful conduct;

s. Whether Plaintiffs and Class Members are entitled to restitution as a result of Samsung's wrongful conduct; and

t. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

263. **Typicality, Fed. R. Civ. P. 23(a)(3).** As to each Class and Subclass, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiffs' PII was in Samsung's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

264. **Adequacy, Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class and their respective State Subclasses because Plaintiffs are members of the Classes and are committed to pursuing this matter against Defendant to obtain relief for the Classes. Plaintiffs have no conflicts of interest with the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Classes' interests.

265. **Superiority and Predominance, Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and

the Classes are relatively small compared to the burden and expense required to individually litigate their claims against Samsung, and thus, individual litigation to redress Samsung's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

266. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Samsung or would be dispositive of the interests of members of the proposed Classes.

267. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Class and Subclasses consist of individuals who provided their PII to Samsung. Class Membership can be determined using Samsung's records.

268. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect Class Members' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

CLAIMS FOR RELIEF ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

269. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

270. Samsung required Plaintiffs and Class Members to submit sensitive PII in order to obtain the full value of Samsung's products and Services or in some instances even to apply for or use the products and Services at all. Samsung also collected and stored sensitive personal information about its customers on its own, either automatically as customers used Samsung's Products and Services, or through third-party data sources.

271. Samsung owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Samsung's security systems to ensure that Plaintiffs' and Class Members' PII in Samsung's possession was properly secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner, (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusion to its networks; and (d) maintaining security measures consistent with industry standards.

272. Samsung's duty to use reasonable care arose from several sources, including but not limited to those described herein.

273. Samsung had common law duties to prevent foreseeable harm to Plaintiffs and Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiffs and Class Members would be harmed by Samsung's failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Samsung

knew that it was more likely than not Plaintiffs and other Class Members would be harmed if it allowed such a breach.

274. Samsung's duty to use reasonable security measures also arose as a result of the special relationship that existed between Samsung, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted Samsung with their PII as part of the purchase of and subsequent use of the products and services Samsung offers as a major consumer electronics company. Samsung alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

275. Samsung's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Samsung. Various FTC publications and data security breach orders further form the basis of Samsung's duty. In addition, individual jurisdictions have enacted statutes based upon the FTC Act that also created a duty.

276. Samsung's duty also arose from Samsung's unique position as one of the largest consumer electronics companies in the world. As a consumer electronics company, Samsung holds itself out as a protector of consumer data, and thereby assumes a duty to reasonably protect the data that was provided to it by Plaintiffs and Class Members. Samsung has stated: "We also recognize the importance of protecting your privacy and information. Our products and services are designed with privacy and security at top of mind."[55] Because of its role as one of the largest

[55] Samsung, *Our Approach to Privacy*, available at https://www.samsung.com/us/account/our-approach-to-privacy/ (last accessed May 19, 2023).

electronics companies, Samsung was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Samsung Data Breach.

277. Samsung admits that it has a responsibility to protect consumer data and that it was entrusted with this data.

278. Samsung knew or should have known that its computing systems and data storage were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

279. Samsung also had a duty to safeguard the PII of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require Samsung to reasonably safeguard sensitive PII, as detailed herein.

280. Samsung was required to provide timely, adequate, and appropriate notification of the Data Breach to Plaintiffs and Class Members. As discussed above, Plaintiffs and Class Members needed timely and effective notice so they could take appropriate measures to prevent, mitigate, or ameliorate the damage caused by Samsung's misconduct. Had they known of the Data Breach earlier and received more detailed information about it, Plaintiffs and Class Members could have taken such measures—including freezing or locking credit profiles, avoiding or reversing unauthorized charges to credit or debit card accounts, cancelling or changing usernames and passwords on compromised accounts, monitoring financial and other accounts and credit reports for fraudulent activity, contacting the banks or other financial institutions that issue their credit or debit cards, obtaining credit monitoring services, and other steps—earlier.

281. Samsung breached the duties it owed to Plaintiffs and Class Members described above and thus was negligent. Samsung breached these duties by, among other things, failing to: (a) exercise reasonable care and implement proper security systems, protocols and practices

sufficient to protect the PII of Plaintiffs and Class Members; (b) detect the Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the PII at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiffs' and Class Members' PII in Samsung's possession had been or was reasonably believed to have been, stolen or compromised.

282. But for Samsung's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised and sold on the dark web.

283. Samsung's failure to take proper security measures to protect the sensitive PII of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' PII.

284. Plaintiffs and Class Members were foreseeable victims of Samsung's inadequate data security practices, and it was also foreseeable that Samsung's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as described in this Complaint.

285. As a direct and proximate result of Samsung's negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach

reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Samsung's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT 2
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)[56]

286. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

287. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Samsung of failing to use reasonable measures to protect PII.

288. The FTC publications and orders also form the basis of Samsung's duty.

289. Samsung violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Samsung's conduct was particularly unreasonable given the nature and amount of PII it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as Samsung including, specifically, the damages that would result to Plaintiffs and Class Members.

290. In addition, under state data security statutes, Samsung had a duty to implement

[56] Plaintiffs do not bring this cause of action on behalf of members of the Arkansas, Louisiana, Maryland, Massachusetts, Oregon, or Rhode Island State Subclasses, or under the laws of those states.

and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

291. Samsung's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

292. Plaintiffs and Class Members are within the class of persons Section 5 of the FTC Act was intended to protect.

293. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

294. Samsung breached its duties to Plaintiffs and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or appropriate computer systems and data security practices that complied with applicable industry standards to safeguard Plaintiffs' and Class Members' PII.

295. Plaintiffs and Class Members were foreseeable victims of Samsung's violations of the FTC Act and state data security statutes. Samsung knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members' PII that complied with applicable industry standards would cause damage to Plaintiffs and Class Members.

296. But for Samsung's violation of the applicable laws and regulations, Plaintiffs' and Class Members' PII would not have been accessed by unauthorized parties.

297. As a direct and proximate result of Samsung's negligence *per se*, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat

of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on illicit markets; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Samsung's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 3
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)[57]

298. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

299. Plaintiffs and Class Members maintained a confidential relationship with Samsung whereby Samsung undertook a duty not to disclose to unauthorized parties the PII that Plaintiffs and Class Members provide to Samsung. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

300. Samsung knew Plaintiffs' and Class Members' PII was disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing

[57] Plaintiffs do not bring this cause of action on behalf of members of the Illinois, Maryland, South Carolina, Washington, or Wisconsin State Subclasses, or under the laws of those states.

to protect the confidentiality and security of the PII it collected, stored, and maintained.

301. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because Samsung failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

302. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

303. But for Samsung's actions and inactions in violation of the parties' understanding of confidence, the PII of Plaintiffs and Class Members would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Samsung's actions and inaction were the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

304. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Samsung's unauthorized disclosure of Plaintiffs' and Class Members' PII. Samsung knew its computer systems and technologies for accepting, securing, and storing Plaintiffs' and Class Members' PII had serious security vulnerabilities because Samsung failed to observe even basic information security practices or correct known security vulnerabilities.

305. As a direct and proximate result of Samsung's breach of confidence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the

compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Samsung's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

306. By collecting and storing this PII and using it for commercial gain, Samsung has a duty of care to use reasonable means to secure and safeguard this PII to prevent disclosure and guard against theft of the PII.

COUNT 4
Breach of Express Contract
(On Behalf of Plaintiffs and the Nationwide Class)

307. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

308. Samsung's Privacy Notice is an agreement between Samsung and individuals who provided their PII to Samsung, including Plaintiffs and Class Members.

309. Although there are some differences among Samsung's Privacy Notices, all state that they apply to "personal information about you" that Samsung obtains "when you interact with [Samsung]," which includes "when you purchase a Samsung product, create a Samsung Account, register or use a Service, contact Customer Support, visit a Samsung retail location, or while attending an event."[58]

[58] https://www.samsung.com/us/account/privacy-policy/ (last accessed May 19, 2023).

310. At all relevant times, including through the date of the Data Breach in July 2022, Samsung's Privacy Policy included the promise that Samsung "maintain[s] safeguards designed to protect personal information [Samsung] obtain[s] through the Services."[59]

311. As described in Paragraphs 195-197, Samsung has repeatedly made other statements to Plaintiffs and Class Members promising to ensure the security of their PII.

312. Samsung further agreed during all relevant times through the date of the Data Breach in July 2022, that it would only share data under certain enumerated circumstances, which include: "if you ask us to do so or otherwise with your consent," "with our subsidiaries and affiliates and with service providers who perform services for us," "with our business partners, such as wireless carriers, as well as third parties who operate apps and services that connect with certain Services," "to law enforcement authorities," "when we believe disclosure is necessary or appropriate to prevent physical harm or financial loss," and to the purchaser or transferee of Samsung's assets in the event that Samsung "sell[s] or transfer[s] all or a portion of [its] business or assets."[60] None of the enumerated circumstances involve sharing Plaintiffs' or Class Members' PII with criminal hackers.

313. Samsung emphasized in its Privacy Policy during all relevant time periods, including through the date of the Data Breach in July 2022, that Samsung "know[s] how important privacy is to [its] customers."[61]

314. Plaintiffs and Class Members on the one side and Samsung on the other formed a

---

[59] *Id*.

[60] *Id*.

[61] Samsung Privacy Policy for the U.S, SAMSUNG, (Dec. 20, 2022), available at https://www.samsung.com/us/account/privacy-policy/ (last accessed May 19, 2023).https://www.samsung.com/us/account/privacy-policy/

contract when Plaintiffs and Class Members obtained products or Services from Samsung, or otherwise provided PII to Samsung subject to its Privacy Policy.

315. Plaintiffs and Class Members fully performed their obligations under the contracts with Samsung.

316. Samsung breached its agreement with Plaintiffs and Class Members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

317. As a direct and proximate result of Samsung's breach of contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Samsung's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 5
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

318. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

319. Plaintiffs and Class Members entered into an implied contract with Samsung when they obtained products or Services from Samsung, or otherwise provided PII to Samsung.

320. As part of these transactions, Samsung agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII was breached or compromised.

321. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Samsung's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiffs and Class Members believed that Samsung would use part of the monies paid to Samsung under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund proper and reasonable data security practices.

322. Plaintiffs and Class Members would not have provided and entrusted their PII to Samsung or would have paid less for Samsung products or Services in the absence of the implied contract or implied terms between them and Samsung. The safeguarding of the PII of Plaintiffs and Class Members was critical to realize the intent of the parties.

323. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Samsung.

324. Samsung breached its implied contracts with Plaintiffs and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect

that information; and (2) disclosed that information to unauthorized third parties.

325. As a direct and proximate result of Samsung's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Samsung's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 6
Unjust Enrichment
(In the alternative)
(On Behalf of Plaintiffs and the Nationwide Class)

326. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

327. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Samsung and that was ultimately stolen in the Samsung Data Breach.

328. Samsung benefitted from the conferral upon it of the PII pertaining to Plaintiffs and

Class Members and by its ability to retain, use, sell, and profit from that information. Samsung understood that it was in fact so benefitted.

329. Samsung also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon Samsung maintaining the privacy and confidentiality of that PII.

330. But for Samsung's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class Members would not have provided their PII to Samsung or would not have permitted Samsung to gather additional PII.

331. Plaintiffs' and Class Members' PII has an independent value to Samsung.

332. Samsung admits that it uses the PII it collects for, among other things, "operat[ing], evaluat[ing], and improv[ing its] business," "developing new products and services," and "conducting market research," and that it uses its PII to "provide ads," which include" targeted (or interest-based) ads."[62]

333. Because of its use of Plaintiffs' and Class Members' PII, Samsung sold more services and products than it otherwise would have. Samsung was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create through the use of Plaintiffs' and Class Members' PII to the detriment of Plaintiffs and Class Members.

334. Samsung also benefitted through its unjust conduct by retaining money paid by Plaintiffs and Class Members that it should have used to provide proper data security to protect Plaintiffs' and Class Members' PII.

335. It is inequitable for Samsung to retain these benefits.

336. As a result of Samsung's wrongful conduct as alleged in this Complaint (including

[62] https://www.samsung.com/us/account/privacy-policy/.

among other things its failure to employ proper data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and Class Members without having proper data security measures, and its other conduct facilitating the theft of that PII), Samsung has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

337. Samsung's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

338. It is inequitable, unfair, and unjust for Samsung to retain these wrongfully obtained benefits. Samsung's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

339. The benefit conferred upon, received, and enjoyed by Samsung was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Samsung to retain the benefit.

340. Samsung's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiffs and Class Members other damages as described herein.

341. Plaintiffs have no adequate remedy at law.

342. Samsung is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Samsung as a result of its wrongful conduct, including specifically: the value to Samsung of the PII that was stolen in the Data Breach; the profits Samsung received and is receiving from the use of that information; the amounts that

Samsung overcharged Plaintiffs and Class Members for use of Samsung's products and services; and the amounts that Samsung should have spent to provide proper data security to protect Plaintiffs' and Class Members' PII.

COUNT 7
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

343. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

344. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

345. An actual controversy has arisen in the wake of the Samsung Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Samsung is currently maintaining data security measures that effectively protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future given the publicity around the Data Breach and the nature and quantity of the PII stored by Samsung.

346. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Samsung continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Samsung continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

347. The Court also should issue corresponding prospective injunctive relief requiring Samsung to employ proper security protocols consistent with law and industry standards to protect consumers' PII.

348. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Samsung. The risk of another such breach is real, immediate, and substantial. If another breach at Samsung occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

349. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Samsung if an injunction is issued. Among other things, if another massive data breach occurs at Samsung, Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Samsung of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Samsung has a pre-existing legal obligation to employ such measures.

350. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Samsung, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

CLAIMS ON BEHALF OF THE ALABAMA SUBCLASS

COUNT 8
Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1, *et seq.*

351. The Alabama Plaintiff identified above ("Plaintiff" for purposes of this Count),

individually and on behalf of the Alabama Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

352. Samsung is a "person" as defined by Ala. Code § 8-19-3(10).

353. Plaintiff and Alabama Subclass Members are "consumers" as defined by Ala. Code § 8-19-3(4).

354. Samsung advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

355. Samsung engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts.

356. Samsung's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate

identified security and privacy risks, and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; and

h. Failing to provide timely and effective notice of the Data Breach as required by Ala. Code 1975, 8-38-2.

357. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

358. Samsung intended to mislead Plaintiff and Alabama Subclass Members and induce

them to rely on its misrepresentations and omissions.

359. Had Samsung disclosed to Plaintiff and Alabama Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

360. Samsung acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Alabama Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

361. As a direct and proximate result of Samsung's deceptive acts and practices, Plaintiff and Alabama Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft, loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

362. Samsung's deceptive acts and practices caused substantial injury to Plaintiff and Alabama Subclass Members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

363. Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including, pursuant to § 8-19-10(a) the greater of (1) actual damages or (2) statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE ALASKA SUBCLASS

COUNT 9
Personal Information Protection Act, Alaska Stat. §§ 45.48.010, *et seq.*

364. The Alaska Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

365. Samsung is a "covered person" as defined in Alaska Stat. § 45.48.090(2) and owns or licenses "personal information" as defined by Alaska Stat. § 45.48.090(7).

366. Plaintiff and Alaska Subclass Members' PII includes PII as covered by Alaska Stat. § 45.48.010(a).

367. Alaska Stat. §§ 45.48.010(a) and (b) required Samsung to accurately notify Plaintiff and Alaska Subclass Members of the Data Breach in the most expeditious time possible and without unreasonable delay.

368. Alaska Stat. § 45.48.010(b) also required Samsung to determine the scope of the breach and restore the reasonable integrity of the information system.

369. By failing to disclose the Data Breach in a timely and accurate manner Samsung violated Alaska Stat. § 45.48.010(b).

370. Pursuant to Alaska Stat. § 45.48.080(b), a violation of Alaska Stat. § 45.48.010(b) is an unfair or deceptive act or practice under the Alaska Consumer Protection Act, Alaska Stat. 45.50.471.

371. As a direct and proximate result of Samsung's violations of Alaska Stat. § 45.48.010(b), Plaintiff and Alaska Subclass Members suffered damages, as described above. Plaintiff and Alaska Subclass Members seek relief measured as the greater of (a) each unlawful act, (b) three times actual damages in an amount to be determined at trial, or (c) statutory damages in the amount of $500 for Plaintiff and each Alaska Subclass Member; reasonable attorneys' fees; and any other just and proper relief available under Alaska Stat. § 45.48.080(b)(2) and Alaska Stat. § 45.50.531.

COUNT 10
Alaska Unfair Trade Practices and Consumer Protection Act
Alaska Stat. § 45-50-471, *et seq*.

372. The Alaska Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if fully set forth herein.

373. Samsung is a "person" within the meaning of Alaska Stat. § 45-50-531(a).

374. Samsung advertised, offered, or sold goods or services in Alaska and engaged in trade or commerce directly or indirectly affecting the people of Alaska.

375. Samsung engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Alaska in the conduct of trade or commerce.

376. Samsung's unfair and deceptive acts and practices included:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Alaska Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and

properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Alaska Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Alaska Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Alaska Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Alaska Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Alaska Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

377. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

378. Samsung intended to mislead Plaintiff and Alaska Subclass Members and induce them to rely on its misrepresentations and omissions.

379. Had Samsung disclosed to Plaintiff and Alaska Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to

continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Alaska Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Alaska Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

380. Samsung acted intentionally, knowingly, and maliciously to violate Alaska's Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiff and Alaska Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

381. As a direct and proximate result of Samsung's unfair and deceptive acts and practices, Plaintiff and Alaska Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

382. Plaintiff and Alaska Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS

COUNT 11
Arizona Consumer Fraud Act, A.R.S. §§ 44-1521, *et seq.*

383. The Arizona Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Arizona Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

384. Samsung is a "person" as defined by A.R.S. § 44-1521(6).

385. Samsung advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

386. Samsung engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A)).

387. Samsung's unfair and deceptive acts and practices included:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of

Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

388. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

389. Samsung intended to mislead Plaintiff and Arizona Subclass Members and induce them to rely on its misrepresentations and omissions.

390. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

391. Samsung acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff's and Arizona Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

392. As a direct and proximate result of Samsung's unfair and deceptive acts and practices, Plaintiff and Arizona Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

393. Plaintiff and Arizona Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS

COUNT 12
Arkansas Deceptive Trade Practices Act
A.C.A. §§ 4-88-101, *et seq.*

394. The Arkansas Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

395. Samsung is a "person" as defined by A.C.A. § 4-88-102(5).

396. Samsung's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

397. Samsung advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

398. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, *et seq*., prohibits unfair, deceptive, false, and unconscionable trade practices.

399. Samsung engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-108(a)(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-108(a)(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services or as to whether goods are original or new or of a particular standard, quality, grade, style, or model;

b. Advertising the goods or services with the intent not to sell them as advertised;

c. Employing bait-and-switch advertising consisting of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell;

d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest;

e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

400. Samsung's unconscionable, false, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy

measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

401. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

402. Samsung intended to mislead Plaintiff and Arkansas Subclass Members and induce

them to rely on its misrepresentations and omissions.

403. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

404. Samsung acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Arkansas Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

405. As a direct and proximate result of Samsung's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass Members' reliance thereon, Plaintiff and Arkansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

406. Plaintiff and the Arkansas Subclass Members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys'

fees and costs.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 13
California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100, *et seq.*

407. The California Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

408. Plaintiffs and Subclass Members are residents of California.

409. Samsung is a corporation organized or operated for the profit or financial benefit of its owners. Samsung collects consumers' personal information ("PII" for purposes of this Count) as defined in Cal. Civ. Code § 1798.140.

410. Samsung violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Samsung's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

411. Samsung has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and Subclass Members' PII. As detailed herein, Samsung failed to do so.

412. As a direct and proximate result of Samsung's acts, Plaintiffs' and Subclass Members' PII, including full names, email addresses, postal addresses, telephone numbers, dates of birth, Social Security numbers, payment card information, and geolocation data, was subjected to unauthorized access and exfiltration, theft, or disclosure.

413. Plaintiffs and Subclass Members seek injunctive or other equitable relief to ensure Samsung hereinafter properly safeguards customers' PII by implementing reasonable security

procedures and practices. Such relief is particularly important because Samsung continues to hold customers' PII, including Plaintiff's and Subclass Members' PII. Plaintiff and Subclass Members have an interest in ensuring that their PII is reasonably protected, and Samsung has demonstrated a pattern of failing to properly safeguard this information, as evidenced by its multiple data breaches.

414. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Samsung and third parties with similar inadequate security measures.

415. On September 13, 2022, counsel for Plaintiff Seirafi provided written notice via certified mail to Samsung at its principal place of business of their intent to pursue claims under the California Consumer Privacy Act and an opportunity for Samsung to cure. The domestic return receipt show that Samsung's letter was received. Plaintiff Seirafi's written notice set forth the violations of Samsung's duty to implement and maintain reasonable security procedures and practices alleged in this Consolidated Complaint.

416. Plaintiff Seirafi's September 13, 2022 written notice, sent in his representative capacity, substantially complied with California Civil Code, Section 1798.150's written notice requirement. In addition, Samsung received written notice of the factual bases of this cause of action and others when plaintiffs in multiple actions that were filed in multiple jurisdictions served Samsung with complaints in connection with the Data Breach. Those complaints were filed more than 90 days ago, prior to the consolidation of the actions in the United States District Court for the District of New Jersey.[63]

[63] These actions included *Seirafi, et al. v. Samsung Electronics Am., Inc.*, No. 3:22-cv-05176 (N.D. Cal.); *Newbery, et al. v. Samsung Electronics Am., Inc.*, No. 1:22-cv-05325 (N.D.

417. These actions contained similar factual allegations to those giving rise to this cause of action, and Samsung has therefore had ample opportunity to investigate the basis of this action and pursue settlement discussions.

418. To date, Samsung has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiff Seirafi's counsel.

419. Plaintiffs and the California Subclass seek statutory damages of between $100 and $750 per customer per violation or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COUNT 14
California Consumer Records Act
Cal. Civ. Code §§ 1798.80, *et seq.*

420. The California Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

421. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information [PII] from unauthorized access, destruction, use, modification,

---

Ill.); *Robinson v. Samsung Electronics Am., Inc.*, No. 2:22-cv-05722 (D.N.J.); *Becker v. Samsung Electronics Am., Inc.*, No. 2:22-cv-05723 (D.N.J.); *DiPaola, et al. v. Samsung Electronics America, Inc.*, No. 2:22-cv-05724; *Fernandez v. Samsung Electronics Am., Inc.*, No. 2:22-cv-05745; *Rollins v. Samsung Electronics Am., Inc.*, No. 2:22-cv-05767 (D.N.J.); and *Mark v. Samsung Electronics Am., Inc.*, C.A. No. 1:22-07974 (S.D.N.Y.); *Gutierrez v. Samsung Electronics America, Inc.*, No. 1:23-cv-00789 (D.N.J.).

or disclosure."

422. Samsung is a business that owns, maintains, and licenses personal information (or "PII"), within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Plaintiffs and California Subclass Members.

423. Businesses that own or license computerized data that includes PII are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of personal information [PII] that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

424. Samsung is a business that owns or licenses computerized data that includes "personal information" [PII] as defined by Cal. Civ. Code § 1798.80.

425. Plaintiffs' and California Subclass Members' PII includes "personal information" as covered by Cal. Civ. Code § 1798.82.

426. Because Samsung reasonably believed that Plaintiffs' and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Samsung had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

427. Samsung failed to fully disclose material information about the Data Breach, including the types of PII impacted.

428. By failing to disclose the Data Breach in a timely and accurate manner, Samsung violated Cal. Civ. Code § 1798.82.

429. Samsung also violated Cal. Civ. Code § 1798.82 by not publishing a notice of data

breach in the format required by Cal. Civ. Code § 1798.82(d)(1).

430. As a direct and proximate result of Samsung's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members suffered damages, as described above.

431. Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 15
California Unfair Competition Act
Cal. Bus. & Prof. Code §§ 17200, *et seq.*

432. The California Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

433. Samsung is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

434. Samsung violated Cal. Bus. & Prof. Code §§ 17200, *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

435. Samsung's "unfair" acts and practices include:

a. Samsung failed to implement and maintain reasonable security measures to protect Plaintiffs' and Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Samsung failed to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and Subclass Members, whose PII has been compromised.

c. Samsung's failure to implement and maintain reasonable security measures

also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

d. Samsung's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of Samsung's grossly inadequate security, consumers could not have reasonably avoided the harms that Samsung caused.

e. Samsung engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

436. Samsung has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

437. Samsung's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Consumer Records Act, Cal. Civ. Code § 1798.80, *et seq.*, and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

h. Failing to provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

438. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

439. As a direct and proximate result of Samsung's unfair, unlawful, and fraudulent acts

and practices, Plaintiffs and California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

440. Samsung acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

441. Plaintiffs and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Samsung's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 16
California Consumer Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq.*

442. The California Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the California Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

443. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing

goods, property or services to consumers primarily for personal, family, or household use.

444. Samsung is a "person" as defined by Civil Code §§ 1761(c) and 1770 and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

445. Plaintiffs and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

446. Samsung's acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the California Subclass Members in violation of Civil Code § 1770, including by:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

447. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

448. Had Samsung disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of

consumers, including Plaintiffs and Subclass Members. Samsung accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

449. On September 13, 2022, counsel for Plaintiff Seirafi provided written notice via certified mail to Samsung at its principal place of business of their intent to pursue claims under the CLRA and an opportunity for Samsung to cure. The domestic return receipt shows that Samsung's letter was received. Plaintiff Seirafi's written notice sets forth the violations of Samsung's duty to implement and maintain reasonable security procedures and practices alleged in this Consolidated Complaint.

450. Plaintiff Seirafi's September 13, 2022 written notice, sent in his representative capacity, substantially complied with California Civil Code, Section 1782's written notice requirement. In addition, Samsung received written notice of the factual bases of this cause of action and others when plaintiffs in multiple actions that were filed in multiple jurisdictions served Samsung with complaints in connection with the Data Breach. Those complaints were filed more than 90 days ago, prior to the consolidation of the actions in the United States District Court for the District of New Jersey.[64]

451. These actions contained similar factual allegations to those giving rise to this cause of action, and Samsung has therefore had ample opportunity to investigate the basis of this action and pursue settlement discussions.

452. To date, Samsung has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiff Seirafi's counsel.

[64] *See* note 61, *supra*.

453. As a direct and proximate result of Samsung's violations of California Civil Code § 1770, Plaintiffs and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

454. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIMS ON BEHALF OF THE COLORADO SUBCLASS

COUNT 17
Colorado Security Breach Notification Act
Colo. Rev. Stat. §§ 6-1-716, *et seq.*

455. The Colorado Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

456. Samsung is a business that owns or licenses computerized data that includes "personal information" [PII] as defined by Colo. Rev. Stat. §§ 6-1-716(1).

457. Plaintiff's and Colorado Subclass Members' PII includes PII as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

458. Samsung is required to accurately notify Plaintiff and Colorado Subclass Members if it becomes aware of a breach of its data security system in the most expedient time possible and

without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

459. Because Samsung was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

460. By failing to disclose the Data Breach in a timely and accurate manner, Samsung violated Colo. Rev. Stat. § 6-1-716(2).

461. As a direct and proximate result of Samsung's violations of Colo. Rev. Stat. § 6- 1-716(2), Plaintiffs and Colorado Subclass Members suffered damages, as described above.

462. Plaintiff and Colorado Subclass Members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

COUNT 18
Colorado Consumer Protection Act
Colo. Rev. Stat. §§ 6-1-101, *et seq.*

463. The Colorado Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

464. Samsung is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

465. Samsung engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

466. Plaintiff and Colorado Subclass Members, as well as the general public, are actual consumers of the products and services offered by Samsung or successors in interest to actual consumers.

467. Samsung engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Making a false representation as to the characteristics of products and

services;

b. Representing that services are of a particular standard, quality, or grade, though Samsung knew or should have known that there were or another;

c. Advertising services with intent not to sell them as advertised;

d. Employing "bait and switch" advertising, which is advertising accompanied by an effort to sell goods, services, or property other than those advertised or on terms other than those advertised; and

e. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

468. Samsung's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

469. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

470. Samsung intended to mislead Plaintiff and Colorado Subclass Members and induce them to rely on its misrepresentations and omissions.

471. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

472. Samsung acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff's and Subclass Members' rights.

Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

473. As a direct and proximate result of Samsung's deceptive trade practices, Plaintiff and Colorado Subclass Members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII, monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

474. Samsung's deceptive trade practices significantly impact the public, because many members of the public are actual or potential consumers of Samsung's services and the Data Breach affected millions of Americans, which include members of the Colorado Subclass.

475. Plaintiff and Colorado Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE CONNECTICUT SUBCLASS

COUNT 19
Connecticut Unfair Trade Practices Act (CUTPA)
C.G.S.A. § 42-110b

476. The Connecticut Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if fully set forth herein.

477. The Connecticut Unfair Trade Practices provides: "No person shall engage in unfair

methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." C.G.S.A. § 42-110b(a).

478. Samsung advertised, offered, or sold goods or services in Connecticut and engaged in trade or commerce directly or indirectly affecting persons in Connecticut.

479. Plaintiff and Connecticut Subclass Members have a private right of action under C.G.S.A. §42-110g(a).

480. As alleged infra, Samsung's actions in violation of the CUTPA include, but are not limited to its failure to disclose the Data Breach in a timely and accurate manner as required by C.G.S.A. § 36a-701b(b) and (c).

481. Specifically, Samsung unreasonably delayed issuing its first public notice to Plaintiff and Connecticut Subclass Members by issuing it over a month after allegedly discovering the Data Breach, while also failing to accurately disclose information accurately, by vaguely referring to the incident in the delayed notice.

482. Samsung's failure to disclose the Data Breach in a timely and accurate manner was misleading to Plaintiff and the Connecticut Subclass as they believed their PII and other private and confidential information was secured by Samsung, as indicated by Samsung's promises of data security and privacy contained in multiple privacy policies and documents, as well as on Samsung's website.

483. Samsung's failure to disclose was material since it affected Plaintiff and Connecticut Subclass Members' decisions, including but not limited to:

a. whether to continue to provide PII or other private and confidential information to Samsung;

b. whether to pay for services to attempt to secure PII compromised by the

data breach;

c. whether to seek the advice of counsel and/or seek legal representation; and

d. whether to continue to use Samsung products and services.

484. Samsung's failure to disclose in a timely and accurate manner was immoral, unethical, oppressive, or unscrupulous since it deprived Plaintiff and Connecticut Subclass Members important knowledge about their compromised PII and delayed any ability they had to try and secure their PII and other private and confidential information.

485. Furthermore, Samsung's failure to disclose in a timely and accurate manner has caused substantial injury to Plaintiff and Connecticut Subclass Members since they were deprived of the knowledge their PII was compromised, and lost a substantial amount of time in which they could have acted to secure their PII in avoidance of: the imminent, impending threats of identity theft, fraud, scams; loss of value of the stolen PII; illegal sales of the compromised PII on the black market; other misuses of their PII; monetary loss and economic harm; the need to pay for mitigation expenses and spend time spent monitoring credit; identity theft insurance costs; credit freezes/unfreezes, time spent initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries due to the Data Breach.

486. Samsung's failure to disclose the Data Breach in a timely and accurate fashion as described above constitutes an unfair or deceptive act or practice in violation of CUTPA, C.G.S.A. § 42-110b.

487. As a result of Samsung's failure to disclose the Data Breach in a timely and accurate fashion Plaintiff and Connecticut Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages including but not limited to fraud and identity theft, time and expenses related to monitoring their

financial accounts for fraudulent activity; an increased, imminent and impending threat of fraud and identity theft, loss of value of their PII, and the value.

488. Additionally, due to Samsung's violation of CUTPA, Samsung is liable for actual damages, equitable relief, punitive damages, as well as reasonable attorneys' fees and costs. C.G.S.A. § 42-110g.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 20
Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq.*

489. The Florida Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

490. Plaintiff and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

491. Samsung advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

492. Samsung engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

493. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

494. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

495. As a direct and proximate result of Samsung's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

496. Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS

COUNT 21
Georgia Fair Business Practices Act
O.C.G.A. §§ 10-1-399, *et seq.*

497. The Georgia Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

498. Samsung, Plaintiff, and Subclass Members are "persons" within the meaning of the Georgia Fair Business Practices Act ("GFBPA"). O.C.G.A. § 10-1- 399(a).

499. Samsung is engaged in, and its acts and omissions affect, trade and commerce under O.C.G.A. § 10-1-392(28). Further, Samsung is engaged in "consumer acts or practices," which are defined as "acts or practices intended to encourage consumer transactions" under O.C.G.A. § 10-1-392(7).

500. Samsung engaged in "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce" in violation of O.C.G.A. § 10-1-393(a). Those acts and practices include those expressly declared unlawful by O.C.G.A. § 10-1-393(b), such as:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

501. In addition, Samsung engaged in the unfair and deceptive acts and practices described below that, while not expressly declared unlawful by O.C.G.A. § 10-1-393(b), are prohibited by O.C.G.A. § 10-1-393(a).

502. In the course of its business, Samsung engaged in unfair acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach; and

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

503. In the course of its business, Samsung also engaged in deceptive acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

c. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

504. The misrepresentations and omissions described in the preceding paragraph were material and made intentionally and knowingly with the intent that Plaintiff and Subclass Members rely upon them in connection with providing to Samsung their extremely sensitive and valuable PII.

505. Samsung knew of the inadequate security controls and vulnerabilities in its data security systems storing Plaintiff and Subclass Members' sensitive and valuable PII, but concealed all of these security failings.

506. Samsung's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiff and Subclass Members, regarding the security and safety of the PII in its care, including the PII of Plaintiff and Subclass Members.

507. Samsung knew or should have known that by collecting, selling, and trafficking in PII, Plaintiff and Subclass Members would reasonably rely upon and assume Samsung's data systems were secure unless Samsung otherwise informed them.

508. Plaintiff and Subclass Members had no effective means on their own to discover the truth. Samsung did not afford Plaintiff and Subclass Members any opportunity to inspect Samsung's data security, learn that it was inadequate and non-compliant with legal requirements, or otherwise ascertain the truthfulness of Samsung's representations and omissions regarding Samsung's ability to protect data and comply with the law.

509. Plaintiff and Subclass Members relied to their detriment upon Samsung's representations and omissions regarding data security, including Samsung's failure to alert customers that its privacy and security protections were inadequate and insecure and thus were vulnerable to attack.

510. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of

protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

511. Samsung acted intentionally, knowingly, and maliciously to violate the GFBPA, and recklessly disregarded Plaintiff and Subclass Members' rights.

512. Samsung's violations present a continuing risk to Plaintiff and Subclass Members, as well as to the general public.

513. Samsung's unlawful acts and practices complained of herein affect the consumer marketplace and the public interest, including the millions of U.S residents and many Georgians affected by the Data Breach.

514. But for Samsung's violations of the GFBPA described above, the Data Breach would not have occurred.

515. As a direct and proximate result of Samsung's violations of the GFBPA, Plaintiff and Subclass Members have suffered injury-in-fact, monetary, and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

516. The GFBPA permits any person who suffers injury or damages as a result of the violation of its provisions to bring an action against the person or persons engaged in such violations. O.C.G.A. § 10-1-399(a).

517. Plaintiff brings this action on behalf of himself and Subclass Members for the relief

requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers and the public at large to make informed decisions related to the security of their sensitive PII, and to protect the public from Samsung's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices.

518. Plaintiff and Subclass Members are entitled to a judgment against Samsung for actual and consequential damages; general, nominal, exemplary, and trebled damages and attorneys' fees pursuant to the GFBPA; costs; and such other further relief as the Court deems just and proper.

COUNT 22
Georgia Uniform Deceptive Practices Act
O.C.G.A. §§ 10-1-370, *et seq.*

519. The Georgia Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

520. Samsung, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

521. Samsung engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

522. Samsung's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's

and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

523. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

524. Samsung intended to mislead Plaintiff and Georgia Subclass Members and induce them to rely on its misrepresentations and omissions.

525. In the course of its business, Samsung engaged in activities with a tendency or capacity to deceive.

526. Samsung acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

527. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Georgia Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

528. As a direct and proximate result of Samsung's deceptive trade practices, Plaintiff and Georgia Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein,

including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

529. Plaintiff and Georgia Subclass Members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT 23
Illinois Personal Information Protection Act
815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

530. The Illinois Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

531. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information (for the purpose of this count, "PII"), Samsung is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

532. Samsung is a Data Collector that owns or licenses computerized data that includes PII. Samsung also maintains computerized data that includes PII which Samsung does not own.

533. Plaintiffs' and Illinois Subclass Members' PII includes "personal information" as defined by 815 Ill. Comp. Stat. § 530/5.

534. Samsung is required to give immediate notice of a breach of a security system to owners of PII which Samsung does not own or license, including Plaintiffs and Illinois Subclass Members, pursuant to 815 Ill. Comp. Stat. § 530/10(b).

535. By failing to give immediate notice to Plaintiffs, Samsung violated 815 Ill. Comp.

Stat. § 530/10(b).

536. Samsung is required to notify Plaintiffs and Illinois Subclass Members of a breach of its data security system which may have compromised PII which Samsung owns or licenses in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

537. By failing to disclose the Data Breach to Plaintiffs and Illinois Subclass Members in the most expedient time possible and without unreasonable delay, Samsung violated 815 Ill. Comp. Stat. § 530/10(a).

538. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

539. As a direct and proximate result of Samsung's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiffs and Illinois Subclass Members suffered damages, as described above.

540. Plaintiffs and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Samsung's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including equitable relief, costs, and attorneys' fees.

COUNT 24
Illinois Consumer Fraud and Deceptive Business Practices Act
815 Ill. Comp Stat. §§ 505, *et seq.*

541. The Illinois Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

542. Samsung is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

543. Plaintiffs and Illinois Subclass Members are "consumers" as defined by 815 Ill.

Comp. Stat. §§ 505/1(e).

544. Samsung's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

545. Samsung's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§

530/10(a);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

546. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

547. Samsung intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

548. The above unfair and deceptive practices and acts by Samsung were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

549. Samsung acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Illinois Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

550. As a direct and proximate result of Samsung's unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer

injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

551. Plaintiffs and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 25
Illinois Uniform Deceptive Trade Practices Act
815 Ill. Comp. Stat. §§ 510/1, *et seq.*

552. The Illinois Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

553. Samsung is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

554. Samsung engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or

misunderstanding.

555. Samsung's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.

556. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

557. The above unfair and deceptive practices and acts by Samsung were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

558. As a direct and proximate result of Samsung's unfair, unlawful, and deceptive trade practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

559. Plaintiffs and Illinois Subclass Members seek all relief allowed by law, including injunctive relief.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 26
Indiana Deceptive Consumer Sales Act
Ind. Code §§ 24-5-0.5-1, *et seq.*

560. The Indiana Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Indiana Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

561. Samsung is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

562. Samsung is a "supplier" as defined by § 24-5-0.5-2(a)(3), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(1).

563. Samsung engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

564. Samsung's representations and omissions include both implicit and explicit representations:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of

Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

565. Samsung's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

566. The injury to consumers from Samsung's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

567. Consumers could not have reasonably avoided injury because Samsung's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Samsung created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

568. Samsung's inadequate data security had no countervailing benefit to consumers or to competition.

569. Samsung's acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Samsung's failure to disclose the inadequacies in its data security interfered with consumers' decision- making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Samsung's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Samsung concerning the state of Samsung security, and because it is functionally impossible for consumers to obtain credit without their PII being in Samsung's systems.

d. Because Samsung took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed below.

570. Samsung also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

571. Samsung intended to mislead Plaintiffs and Indiana Subclass Members and induced them to rely on its misrepresentations and omissions.

572. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

573. Had Samsung disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

574. Samsung had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the PII in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Samsung and Plaintiffs and the Indiana Subclass as described herein. In addition, such a duty is

implied by law due to the nature of the relationship between consumers – including Plaintiffs and the Indiana Subclass – and Samsung, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Samsung. Samsung's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Indiana Subclass that contradicted these representations.

575. Samsung acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiffs' and Indiana Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate. Samsung's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

576. Despite receiving notice, Samsung has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

577. Samsung's conduct includes incurable deceptive acts that Samsung engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5- 0.5-2(a)(8).

578. As a direct and proximate result of Samsung's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiffs and Indiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-

monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

579. Samsung's violations present a continuing risk to Plaintiffs and Indiana Subclass Members as well as to the general public.

580. Plaintiffs and Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT 27
Iowa Private Right of Action for Consumer Frauds Act
Iowa Code § 714H

581. The Iowa Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and realleges the allegations set forth in paragraphs 1 through 268 and incorporates the same as if fully set forth herein.

582. Samsung is a "person" as defined by Iowa Code § 714H.2(7).

583. Plaintiff and Iowa Subclass Members are "consumers" as defined by Iowa Code § 714H.2(3).

584. Samsung's conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), & (8).

585. Samsung engaged in unfair, deceptive, and unconscionable trade practices, in

violation of the Iowa Private Right of Action for Consumer Frauds Act, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Iowa Personal Information Security Breach Protection Law, Iowa Code § 715C.2, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Iowa Personal Information Security Breach Protection Law, Iowa Code § 715C.2;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the

Iowa Personal Information Security Breach Protection Law, Iowa Code § 715C.2.

586. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

587. Samsung intended to mislead Plaintiff and Iowa Subclass Members and induced them to rely on its misrepresentations and omissions.

588. Samsung acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff's and Iowa Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

589. Because of Samsung's unfair, deceptive, and unconscionable conduct, Plaintiff and Iowa Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach. But for Samsung's actions and omissions, Plaintiff and Subclass Members would not have suffered these injuries.

590. Plaintiff will provide the requisite notice to the Iowa Attorney General pursuant to Iowa Code § 714H.7.

591. Plaintiff and Iowa Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT 28
Protection of Consumer Information
Kan. Stat. Ann. §§ 50-7a02(a), *et seq.*

592. The Kansas Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Kansas Subclass repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

593. Samsung is a person that conducts business in Kansas that owns or licenses computerized data that includes PII as defined by Kan. Stat. Ann. § 50-7a02(a).

594. Plaintiff's and Kansas Subclass Members' personal information (for the purpose of this count, "PII") includes "personal information" as covered under Kan. Stat. Ann. § 50-7a02(a).

595. Samsung is required to accurately notify Plaintiff and Kansas Subclass Members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass Members' PII, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

596. Because Samsung was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass Members' PII, Samsung had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

597. By failing to disclose the Data Breach in a timely and accurate manner, Samsung violated Kan. Stat. Ann. § 50-7a02(a).

598. As a direct and proximate result of Samsung's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass Members suffered damages, as described above.

599. Plaintiff and Kansas Subclass Members seek relief under Kan. Stat. Ann. § 50-

7a02(g), including equitable relief.

COUNT 29
Kansas Consumer Protection Act
K.S.A. §§ 50-623, *et seq.*

600. The Kansas Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

601. K.S.A. §§ 50-623, *et seq*. is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

602. Plaintiff and Kansas Subclass Members are "consumers" as defined by K.S.A. § 50-624(b).

603. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

604. Samsung is a "supplier" as defined by K.S.A. § 50-624(l).

605. Samsung advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

606. Samsung engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the

security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b; and

h. Omitting, suppressing, and concealing the material fact that it did not implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach.

607. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

608. Samsung intended to mislead Plaintiff and Kansas Subclass Members and induce

them to rely on its misrepresentations and omissions.

609. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

610. Samsung also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Samsung knew were substantially one-sided in favor of Samsung (see K.S.A. § 50- 627(b)(5)).

611. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their PII in Samsung's possession.

612. The above unfair, deceptive, and unconscionable practices and acts by Samsung were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

613. Samsung acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff's and Kansas Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

614. As a direct and proximate result of Samsung's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

615. Plaintiffs will provide notice of this action to the Attorney General of Kansas.

616. Plaintiff and Kansas Subclass Members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS

COUNT 30
Database Security Breach Notification Law
La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.*

617. The Louisiana Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

618. Samsung is a business that owns or licenses computerized data that includes PII as

defined by La. Rev. Stat. Ann. § 51:3074(C).

619. Plaintiff's and Louisiana Subclass Members' PII includes PII as covered under La. Rev. Stat. Ann. § 51:3074(C).

620. Samsung is required to accurately notify Plaintiff and Louisiana Subclass Members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass Members' PII, in the most expedient time possible and without unreasonable delay. La. Rev. Stat. Ann. § 51:3074(C).

621. Because Samsung was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass Members' PII, Samsung had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

622. By failing to disclose the Data Breach in a timely and accurate manner, Samsung violated La. Rev. Stat. Ann. § 51:3074(C).

623. As a direct and proximate result of Samsung's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass Members suffered damages, as described above.

624. Plaintiff and Louisiana Subclass Members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

COUNT 31
Louisiana Unfair Trade Practices and Consumer Protection Law
La. Rev. Stat. Ann. §§ 51:1401, *et seq.*

625. The Louisiana Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

626. Samsung, Plaintiff, and the Louisiana Subclass Members are "persons" within the

meaning of the La. Rev. Stat. Ann. § 51:1402(8).

627. Plaintiff and Louisiana Subclass Members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

628. Samsung engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

629. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

630. Samsung engaged in unfair and deceptive acts and practices that violated La. Rev. Stat. Ann. § 51:1405, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII;

g. Failing to provide timely and accurate notice of the Data Breach as required by the Database Security Breach Notification Law, La. Stat. Ann. § 51:3071, *et seq*.; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

631. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

632. Samsung intended to mislead Plaintiff and Louisiana Subclass Members and induce them to rely on its misrepresentations and omissions.

633. Samsung's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Louisiana Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

634. Samsung acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

635. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

636. As a direct and proximate result of Samsung's unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

637. Plaintiff and Louisiana Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Samsung's knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS

COUNT 32
Maryland Consumer Protection Act
Md. Comm. Code §§ 13-301, *et seq.*

638. The Maryland Plaintiff identified above ("Plaintiff" for purposes of this Count),

individually and on behalf of the Maryland Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

639. Samsung is a person as defined by Md. Comm. Code § 13-101(h).

640. Samsung's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

641. Maryland Subclass Members are "consumers" as defined by Md. Comm. Code § 13-101(c).

642. Samsung advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d)(2).

643. Samsung advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

644. Samsung engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Representing that consumer goods or services have a characteristic or benefit that they do not have;

c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;

d. Failing to state a material fact where the failure deceives or tends to deceive;

e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

f. Deception, fraud, false pretense, false premise, misrepresentation, or

knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

645. Samsung engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland PII Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland PII Protection Act, Md. Comm. Code § 14-3503;

f. Omitting, suppressing, and concealing the material fact that it did not

properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland PII Protection Act, Md. Comm. Code § 14-3503.

646. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII. Samsung's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

647. Samsung intended to mislead Plaintiff and Maryland Subclass Members and induce them to rely on its misrepresentations and omissions.

648. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

649. Samsung acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff and Maryland Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

650. As a direct and proximate result of Samsung's unfair and deceptive acts and practices, Plaintiff and Maryland Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

651. Plaintiff and Maryland Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS

COUNT 33
Massachusetts Consumer Protection Act
Mass. Gen. Laws. Ann. Ch. 93A, §§ 1, *et seq.*

652. The Massachusetts Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

653. Samsung and Massachusetts Subclass Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

654. Samsung operates in "trade" or "commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

655. Samsung advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as

defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

656. Samsung engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Omitting, suppressing, and concealing the material fact that it did not

properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

657. Samsung's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Samsung solely held the true facts about its inadequate security for PII, which Plaintiff and the Massachusetts Subclass Members could not independently discover.

658. Consumers could not have reasonably avoided injury because Samsung's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Samsung created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

659. Samsung's inadequate data security had no countervailing benefit to consumers or to competition.

660. Samsung intended to mislead Plaintiff and Massachusetts Subclass Members and induce them to rely on its misrepresentations and omissions. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

661. Samsung acted intentionally, knowingly, and maliciously to violate Massachusetts' Consumer Protection Act, and recklessly disregarded Plaintiff and Massachusetts Subclass

Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

662. As set forth in paragraphs 420-421 above, Plaintiff has substantially complied with the notice requirements of Mass. Gen. Laws Ann. Ch. 93A, § 9(3). In addition, Samsung received written notice of the factual bases of this cause of action and others when plaintiffs in multiple actions that were filed in multiple jurisdictions served Samsung with complaints in connection with the Data Breach. Those complaints were filed more than 90 days ago, prior to the consolidation of the actions in the United States District Court for the District of New Jersey.[65]

663. These actions contained similar factual allegations to those giving rise to this cause of action, and Samsung has therefore had ample opportunity to investigate the basis of this action and pursue settlement discussions.

664. To date, Samsung has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiff's counsel.

665. As a direct and proximate result of Samsung's unfair and deceptive, Plaintiff and Massachusetts Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

666. Plaintiff and Massachusetts Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or

[65] *See* note 61, *supra.*

other equitable relief, and attorneys' fees and costs.

COUNT 34
Massachusetts Privacy Statute
Mass. Gen. Laws Ch. 214, §1B

667. The Massachusetts Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if fully set forth herein.

668. Mass. Gen. Laws ch. 214, §1B provides that "a person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages." Mass. Gen. Laws ch. 214, § 1B.

669. The statute is framed "in broad terms so that the courts can develop the law thereunder on a case-by-case basis, by balancing relevant factors," including "the location of the intrusion, the means used, the frequency and duration of the intrusion, and the underlying purpose behind the intrusion." *Wofse v. Horn*, 523 F. Supp. 3d 122, 137 (D. Mass. 2021).

670. Plaintiff and Massachusetts Subclass Members reasonably expected that the PII they shared with Samsung would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

671. Samsung intentionally intruded into Plaintiff's and Massachusetts Subclass Members' seclusion by disclosing without permission their PII to a third party who then sold their PII to other third parties on the dark web.

672. By failing to keep Plaintiff's and Massachusetts Subclass Members' PII secure, and

disclosing PII to unauthorized parties for unauthorized use, Samsung unlawfully invaded Plaintiff's and Massachusetts Subclass Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII that was properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to properly secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

673. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII.

674. Samsung's intrusions into Plaintiff's and Massachusetts Subclass Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

675. As a direct and proximate result of Samsung's invasions of privacy, Plaintiff and Massachusetts Subclass Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among

other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Samsung; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Samsung's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 35
Michigan Consumer Protection Act
Mich. Comp. Laws Ann. §§ 445.903, *et seq.*

676. The Michigan Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

Samsung and Michigan Subclass Members are "persons" as defined by Mich. Comp. Laws Ann. § 445.902(d).

677. Samsung advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.902(g).

678. Samsung engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter.

679. Samsung's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. § 445.72, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties

imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. § 445.72, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. § 445.72, *et seq.*

680. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

681. Samsung intended to mislead Plaintiff and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

682. Samsung acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff's and Michigan Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

683. As a direct and proximate result of Samsung's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value

of access to their PII; and the value of identity protection services made necessary by the Data Breach.

684. Plaintiff and Michigan Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS

COUNT 36
Minnesota Consumer Fraud Act
Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.*

685. The Minnesota Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

686. Samsung, Plaintiff, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

687. Samsung's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

688. Samsung engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

689. Samsung engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and

sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

690. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

691. Samsung intended to mislead Plaintiff and Minnesota Subclass Members and induce them to rely on its misrepresentations and omissions.

692. Samsung's fraudulent, misleading, and deceptive practices affected the public interest, including the many Minnesotans affected by the Data Breach.

693. As a direct and proximate result of Samsung's fraudulent, misleading, and deceptive practices, Plaintiff and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

694. Plaintiff and Minnesota Subclass Members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT 37
Minnesota Uniform Deceptive Trade Practices Act
Minn. Stat. §§ 325D.43, *et seq.*

695. The Minnesota Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

696. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Samsung violated Minn. Stat. § 325D.44, including the following provisions:

a. Representing that its goods and services had characteristics, uses, and benefits that they did not have;

b. Representing that goods and services are of a particular standard or quality when they are of another;

c. Advertising goods and services with intent not to sell them as advertised;

d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding.

697. Samsung's deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's

and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

698. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

699. Samsung intended to mislead Plaintiff and Minnesota Subclass Members and induce them to rely on its misrepresentations and omissions.

700. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

701. Samsung acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Minnesota Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

702. As a direct and proximate result of Samsung's deceptive trade practices, Plaintiff and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft;

loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

703. Plaintiff and Minnesota Subclass Members seek all relief allowed by law, including injunctive relief and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEVADA SUBCLASS

COUNT 38
Nevada Consumer Fraud Act
Nev. Rev. Stat. §§ 41.600, *et seq*.

704. The Nevada Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if fully set forth herein.

705. Samsung is a "person" under the Nevada Consumer Fraud Act.

706. Nev. Rev. Stat. § 41.600 provides that "[a]n action may be brought by any person who is a victim of consumer fraud," including "a deceptive trade practice as defined in NRS § 598.0915 to 598.025, inclusive."

707. Samsung engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including:

a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale, in violation of Nev. Rev. Stat. § 598.0915(5);

b. Representing that goods or services for sale are of a particular standard, quality, or grade when Samsung knew or should have known that they are of another standard, quality, or grade, in violation of Nev. Rev. Stat. § 598.0915(7);

c. Advertising goods or services with intent not to sell them as advertised, in violation of Nev. Rev. Stat § 598.0915(9);

d. Knowingly making any other false representation in a transaction, in violation of Nev. Rev. Stat § 598.0915(15);

e. Failing to disclose a material fact in connection with the sale of goods or services, in violation of Nev. Rev. Stat. § 598.0923(A)(2); and

f. Violating state and federal statutes or regulations relating to the sale of goods or services, in violation of Nev. Rev. Stat. § 598.0923(1)(c).

708. Samsung's deceptive trade practices in the course of its business include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Nevada Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Nevada Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Nevada Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Nevada Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not

properly secure Plaintiff's and Nevada Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Nevada Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

709. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

710. Had Samsung disclosed to Plaintiff and Nevada Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Nevada Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Nevada Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

711. Samsung acted intentionally, knowingly, and maliciously to violate Nevada's Consumer Fraud Act, and recklessly disregarded Plaintiff's and Nevada Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

712. As a direct and proximate result of Samsung's deceptive trade practices, Plaintiff and Nevada Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein,

including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

713. Plaintiff and Nevada Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs available under Nev. Rev. Stat. § 41.600(3).

COUNT 39
Nevada Deceptive Trade Practices Act
Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.*

714. The Nevada Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

715. Samsung advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

716. Samsung engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including:

a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5);

b. Representing that goods or services for sale are of a particular standard, quality, or grade when Samsung knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);

c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat § 598.0915(9);

d. Knowingly making any other false representation in a transaction in violation of Nev. Rev. Stat § 598.0915(15);

e. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(1)(b); and

f. Violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(1)(c).

717. Samsung's deceptive trade practices in the course of its business include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not

properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

718. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

719. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

720. Samsung acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

721. As a direct and proximate result of Samsung's deceptive trade practices, Plaintiff and Nevada Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their

financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

722. Plaintiff and Nevada Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS

COUNT 40
Notice of Security Breach
N.H. Rev. Stat. §§ 359-C:20(I)(A), *et seq.*

723. The New Hampshire Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

724. Samsung is a business that owns or licenses computerized data that includes PII as defined by N.H. Rev. Stat. § 359-C:20(I)(a).

725. Plaintiff's and New Hampshire Subclass Members' PII includes PII as covered under N.H. Rev. Stat. § 359-C:20(I)(a).

726. Samsung is required to accurately notify Plaintiff and New Hampshire Subclass Members if Samsung becomes aware of a breach of its data security system in which misuse of PII has occurred or is reasonably likely to occur, as soon as possible under N.H. Rev. Stat. § 359-C:20(I)(a).

727. Because Samsung was aware of a security breach in which misuse of PII has occurred or is reasonably likely to occur, Samsung had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. § 359-C:20(I)(a).

728. By failing to disclose the Data Breach in a timely and accurate manner, Samsung violated N.H. Rev. Stat. § 359-C:20(I)(a).

729. As a direct and proximate result of Samsung's violations of N.H. Rev. Stat. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass Members suffered damages, as described above.

730. Plaintiff and New Hampshire Subclass Members seek relief under N.H. Rev. Stat. § 359-C:21(I), including actual damages and injunctive relief.

COUNT 41
New Hampshire Consumer Protection Act
N.H. Rev. Stat. §§ 358-A:1, *et seq.*

731. The New Hampshire Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 and incorporates the same as if set forth herein.

732. Samsung is a "person" under the New Hampshire Consumer Protection Act.

733. Samsung advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H. Rev. Stat. § 358-A:1.

734. Samsung engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H. Rev. Stat. § 358-A:2, including:

a. Representing that its goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that its goods or services are of a particular standard or quality if they are of another;

c. Advertising its goods or services with intent not to sell them as advertised.

735. Samsung's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

736. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to

protect the confidentiality of consumers' PII.

737. Samsung acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiff and New Hampshire Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate. Samsung's acts and practices went beyond the realm of strictly private transactions.

738. As a direct and proximate result of Samsung's unfair and deceptive acts and practices, Plaintiff and New Hampshire Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

739. Plaintiff and New Hampshire Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 42
New Jersey Consumer Fraud Act
N.J. S.A. §§ 56:8-1, *et seq.*

740. The New Jersey Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 and incorporate the same as if set forth herein.

741. Samsung is a "person," as defined by N.J.S.A. § 56:8-1(d).

742. Samsung sells "merchandise," as defined by N.J.S.A. § 56:8-1(c) & (e).

743. The New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. §§ 56:8-2 prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

744. New Jersey CFA claims for unconscionable commercial practice need not allege any fraudulent statement, representation, or omission by the defendant. *See Dewey v. Volkswagen AG*, 558 F. Supp. 2d 505, 525 (D.N.J. 2008); *see also Cox v. Sears Roebuck & Co*., 138 N.J. 2, 19 (1994).

745. "The standard of conduct that the term 'unconscionable' implies is lack of 'good faith, honesty in fact and observance of fair dealing.'" *Cox*, 138 N.J. 2 at 18 (quoting *Kugler v. Romain*, 58 N.J. 522, 544 (1971)). "In addition, '[i]ntent is not an essential element' for allegations related to unconscionable commercial practices to succeed." *Fenwick v. Kay Am. Jeep, Inc.,* 72 N.J. 372, 379 (1977).

746. Samsung's handling and treatment of Plaintiffs' and Subclass Members' PII was unconscionable because:

a. Plaintiffs and Subclass Members had no choice but to provide their PII to Samsung in order to use their Samsung products.

b. To the extent that written contracts exist between Plaintiffs and Subclass Members on the one hand and Samsung on the other hand, those written contracts were written by Samsung and were not negotiable.

c. Once Plaintiffs and Subclass Members provided their PII to Samsung, protection of that PII was solely in Samsung's control. There is no way for Plaintiffs and Subclass Members to take any reasonable steps on their own to protect the PII in Samsung's hands, nor is there any way that Plaintiffs and Subclass Members would have any knowledge that it would be necessary for them to take steps on their own to protect their PII.

d. Samsung had had prior data security breaches and, thus, knew or should have known that its data security was inadequate and needed to take additional security measures to protect Plaintiffs' and Subclass Members' PII, but failed to do so, even though Samsung was the only entity in a position to protect Plaintiffs' and Subclass Members PII from wrongdoers.

e. Once Samsung became aware of the security breach, it failed to notify Plaintiffs and Subclass Members of the breach, thus depriving them the opportunity to take measures to protect themselves from the effects of Samsung's failure to protect their PII.

f. Samsung's practices for handing and protecting Plaintiffs' and Subclass Members' PII was contrary to public policy in that Samsung failed to follow FTC guidelines with respect to the protection of PII and otherwise failed to follow industry standards for providing reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

747. Samsung's handling and treatment of Plaintiffs' and Subclass Members' PII was deceptive because Samsung:

a. Misrepresented that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

b. Misrepresented that it would comply with common law and statutory duties

pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163, *et seq.*;

c. Omitted, suppressed, and concealed the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

d. Omitted, suppressed, and concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163, *et seq*.

748. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

749. Samsung intended to mislead Plaintiffs and Subclass Members and induce them to rely on its omissions of material fact.

750. Samsung acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

751. As a direct and proximate result of Samsung's unconscionable and deceptive practices, Plaintiffs and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud

and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

752. Plaintiffs and Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS

COUNT 43
New Mexico Unfair Practices Act
N.M. Stat. Ann. §§ 57-12-2, *et seq.*

753. The New Mexico Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

754. Samsung is a "person" as meant by N.M. Stat. Ann. § 57-12-2.

755. Samsung was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

756. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

757. Samsung engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce in violation of N.M. Stat. § 57-12-2, including the following:

a. Representing that its goods and services have approval, characteristics,

benefits, or qualities that they do not have;

b. Representing that its goods and services are of a particular standard or quality when they are of another;

c. Using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive;

d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff's and the New Mexico Subclass' detriment;

e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment.

758. Samsung's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico laws mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable

security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes and mandating reasonable data security, N.M. Stat. § 57-12C-4;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes mandating reasonable data security, N.M. Stat. § 57-12C-4.

759. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

760. Samsung intended to mislead Plaintiff and New Mexico Subclass Members and induce them to rely on its misrepresentations and omissions.

761. Samsung acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

762. As a direct and proximate result of Samsung's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-

monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

763. Plaintiff and New Mexico Subclass Members seek all monetary and non- monetary relief allowed by law, including pursuant to N.M. Stat. Ann. § 57-12-10, injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 44
New York General Business Law
N.Y. Gen. Bus. Law §§ 349, *et seq.*

764. The New York Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the New York Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

765. Samsung engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

766. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

767. Samsung acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

768. As a direct and proximate result of Samsung's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer

injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

769. Samsung's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

770. The above deceptive and unlawful practices and acts by Samsung caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

771. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT 45
North Carolina Identity Theft Protection Act
N.C. Gen. Stat. §§ 75-60, *et seq.*

772. The North Carolina Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

773. Samsung is a business that owns or licenses computerized data that includes

personal information (for the purpose of this count, "PII"), as defined by N.C. Gen. Stat. § 75-61(1).

774. Plaintiff and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

775. Samsung is required to accurately notify Plaintiff and North Carolina Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

776. Plaintiff's and North Carolina Subclass Members' PII includes PII as covered under N.C. Gen. Stat. § 75-61(10).

777. Because Samsung discovered a security breach and had notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), Samsung had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

778. By failing to disclose the Data Breach in a timely and accurate manner, Samsung violated N.C. Gen. Stat. § 75-65.

779. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

780. As a direct and proximate result of Samsung's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass Members suffered damages, as described above.

781. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorneys' fees.

COUNT 46
North Carolina Unfair Trade Practices Act
N.C. Gen. Stat. Ann. §§ 75-1.1., *et seq.*

782. The North Carolina Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

783. Samsung advertised, offered, or sold goods or services in North Carolina and engaged in commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

784. Samsung engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

785. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

786. Samsung intended to mislead Plaintiff and North Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

787. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

788. Samsung acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina

Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

789. As a direct and proximate result of Samsung's unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

790. Samsung's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

791. Plaintiff and North Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 47
Ohio Consumer Sales Practices Act
Ohio Rev. Code §§ 1345.01, *et seq.*

792. The Ohio Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

793. Plaintiffs are "persons," as defined by Ohio Rev. Code § 1345.01(B).

794. Samsung was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

795. Samsung advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

796. Samsung engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.02, including:

a. Representing that the subject of a transaction had approval, performance characteristics, uses, and benefits that it did not have;

b. Representing that the subject of a transaction was of a particular standard or quality when they were not.

797. Samsung engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiffs to reasonably protect their interest because of their ignorance of the issues discussed herein;

b. Knowing at the time the consumer transaction was entered into of the inability of the consumer to receive a substantial benefit from the subject of the consumer transaction;

c. Requiring the consumer to enter into a consumer transaction on terms the supplier knew were substantially one-sided in favor of the supplier;

d. Knowingly making a misleading statement of opinion on which the consumer was likely to rely to the consumer's detriment.

798. Samsung's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy

measures to protect Plaintiffs' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

799. Samsung's representations and omissions were material because they deceived Plaintiffs, and were likely to deceive other reasonable consumers, about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

800. Samsung intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions.

801. Samsung acted intentionally, knowingly, and maliciously to violate Ohio's

Consumer Sales Practices Act, and recklessly disregarded Plaintiffs' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

802. Samsung's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the Data Breach.

803. As a direct and proximate result of Samsung's unfair, deceptive, and unconscionable acts and practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non- monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

804. Pursuant to Ohio Rev. Code § 1345.09(A), each Plaintiff, individually, seeks actual economic damages and non-economic damages of up to five thousand dollars.

805. Pursuant to § Ohio Rev. Code 1345.09(D), Plaintiffs seek declaratory and injunctive relief.

806. Pursuant to Ohio Rev. Code § 1345.09(F), Plaintiffs seek an award of reasonable attorneys' fees.

COUNT 48
Ohio Deceptive Trade Practices Act
Ohio Rev. Code §§ 4165.01, *et seq.*

807. The Ohio Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

808. Samsung, Plaintiffs, and Ohio Subclass Members are "persons" as defined by Ohio

Rev. Code § 4165.01(D).

809. Samsung advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

810. Samsung engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality when they are of another;

c. Advertising its goods and services with intent not to sell them as advertised.

811. Samsung's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

812. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

813. Samsung intended to mislead Plaintiffs and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

814. Samsung acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Ohio Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

815. As a direct and proximate result of Samsung's deceptive trade practices, Plaintiffs and Ohio Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and

the value of identity protection services made necessary by the Data Breach.

816. Plaintiffs and Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

COUNT 49
Oklahoma Consumer Protection Act
Okla. Stat. Tit. 15, §§ 751, *et seq.*

817. The Oklahoma Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

818. Samsung is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

819. Samsung's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

820. Samsung, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

a. Making false or misleading representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions;

b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another;

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised;

d. Committing deceptive trade practices that deceived or could reasonably be

expected to deceive or mislead a person to the detriment of that person as defined by section 752(13);

e. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14).

821. Samsung's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

822. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

823. Samsung intended to mislead Plaintiff and Oklahoma Subclass Members and induce them to rely on its misrepresentations and omissions.

824. Had Samsung disclosed to Plaintiff and Oklahoma Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Oklahoma Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Oklahoma Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

825. The above unlawful practices and acts by Samsung were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and the Oklahoma Subclass Members.

826. Samsung acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy

protections were inadequate.

827. As a direct and proximate result of Samsung's unlawful practices, Plaintiff and Oklahoma Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

828. Plaintiff and Oklahoma Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OREGON SUBCLASS

COUNT 50
Oregon Unlawful Trade Practices Act
Or. Rev. Stat. §§ 646.605, *et seq.*

829. The Oregon Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

830. Samsung is a "person," as defined by Or. Rev. Stat. § 646.605(4).

831. Samsung engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

832. Samsung sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

833. Samsung advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

834. Oregon engaged in unlawful practices in the course of its business and occupation,

in violation of Or. Rev. Stat. § 646.608, included the following:

a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Advertising its goods or services with intent not to provide them as advertised;

d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect.

835. Samsung's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, et seq., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.

836. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

837. Samsung intended to mislead Plaintiff and Oregon Subclass Members and induce them to rely on its misrepresentations and omissions.

838. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

Samsung acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

839. As a direct and proximate result of Samsung's unlawful practices, Plaintiff and Oregon Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

840. Plaintiff and Oregon Subclass Members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 51
Pennsylvania Unfair Trade Practices And Consumer Protection Law
73 Pa. Cons. Stat. §§ 201-1, *et seq.*

841. The Pennsylvania Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

842. Samsung is a "person," as meant by 73 Pa. Cons. Stat. § 201-2(2).

843. Plaintiff and Pennsylvania Subclass Members purchased goods and services in

"trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

844. Samsung engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

845. Samsung's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable

security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

846. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

847. Samsung intended to mislead Plaintiff and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

848. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

849. Samsung acted intentionally, knowingly, and maliciously to violate Pennsylvania

Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

850. As a direct and proximate result of Samsung's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass Members' reliance on them, Plaintiff and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

851. Plaintiff and Pennsylvania Subclass Members seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS

COUNT 52
Rhode Island Deceptive Trade Practices Act
R.I. Gen. Laws §§ 6-13.1, *et seq.*

852. The Rhode Island Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Rhode Island Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

853. Plaintiff and Rhode Island Subclass Members are each a "person," as defined by R.I. Gen. Laws § 6-13.1-1(3).

854. Plaintiff and Rhode Island Subclass Members purchased goods and services for personal, family, or household purposes.

855. Samsung advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

856. Samsung engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including:

a. Representing that its goods and services have approval, characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-1(6)(v));

b. Representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-1(6)(vii));

c. Advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-1(6)(ix));

d. Engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-1(6)(xii));

e. Engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-1(6)(xiii)); and

f. Using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-1(6)(xiv)).

857. Samsung's unfair and deceptive acts include:

a. Failing to implement and maintain reasonable security and privacy

measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2.

858. Samsung's representations and omissions were material because they were likely

to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

859. Samsung intended to mislead Plaintiff and Rhode Island Subclass Members and induce them to rely on its misrepresentations and omissions.

860. Samsung acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Rhode Island Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

861. As a direct and proximate result of Samsung's unfair and deceptive acts, Plaintiff and Rhode Island Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

862. Plaintiff and Rhode Island Subclass Members seek all monetary and non-monetary relief allowed by law, including, pursuant to R.I. Gen. Laws § 6-13.1-5.2, actual damages or statutory damages of $500 per Subclass Member (whichever is greater), punitive damages, injunctive relief, other equitable relief, and attorneys' fees and costs.

COUNT 53
Right to Privacy
R.I. Gen. Laws Section 9-1-28.1

863. The Rhode Island Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Rhode Island Subclass, repeats and realleges the factual

allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

864. Samsung advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting persons in Rhode Island.

865. During the course of engaging in trade or commerce with persons in Rhode Island, Samsung engaged in acts in violation of Plaintiff's and Rhode Island Subclass Members' Rights to Privacy, including but not limited to the right to be secure from unreasonable intrusion upon one's physical solitude or seclusion; and the right to be secure from unreasonable publicity given to one's private life. R.I. Gen. Laws § 9-1-28.1(a)(1) & (3).

866. R.I. Gen. Laws § 9-1-28.1 [P.L. 1980, ch. 403 § 1, codified as G.L. 1956 § 9-1-28.1 has made it "the policy of this state that every person in this state shall have a right to privacy." *See Pontbriand v. Sundlun*, 699 A.2d 856, 863 (R.I. 1997).

867. Plaintiff and Rhode Island Subclass Members have a private right of action under Rhode Island Right to Privacy law. Pursuant to R.I. Gen. Laws § 9-1-28.1(b), it states, in relevant part, that "[e]very person who subjects or causes to be subjected any citizen of this state or other person within the jurisdiction thereof to a deprivation and/or violation of his or her right to privacy shall be liable to the party injured in an action at law, suit in equity, or any other appropriate proceedings for redress in either the superior court or district court of this state."

868. Plaintiff and Rhode Island Subclass Members reasonably and actually expected that the PII they shared with Samsung would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

869. Samsung intentionally intruded into Plaintiff's and Rhode Island Subclass

Members' seclusion by disclosing without permission their PII to a third party.

870. By failing to keep Plaintiff's and Rhode Island Subclass Members' PII secure, and by disclosing PII to unauthorized parties for unauthorized use, Samsung unlawfully invaded Plaintiff's Rhode Island Subclass Members' rights to privacy to seclusion by, *inter alia*:

a. Invading into their private lives in a manner that is offensive or objectionable to a reasonable man;

b. Failing to sufficiently secure their private PII from disclosure to unauthorized persons by making sure Samsung's data systems were not vulnerable to attack and were in accordance with FTC and industry standards;

c. Invading their privacy by improperly using their PII that was properly obtained for a specific purpose or another purpose, or disclosing it to unauthorized persons;

d. Allowing for the publication of PII and other private information to unauthorized persons in a manner which is offensive or objectionable to a reasonable man of ordinary sensibilities; and

e. Enabling the disclosure of their PII without their consent.

871. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII.

872. Samsung's intrusions into Plaintiff's and Rhode Island Subclass Members' seclusion were substantial and would be offensive and objection to reasonable people.

873. As a direct and proximate result of Samsung's invasions of privacy, Plaintiff and the Rhode Island Subclass Members have been injured and are entitled to reasonable attorneys' fees and costs pursuant to R.I. Gen. Laws § 9-1-28.1(b).

CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS

COUNT 54
South Carolina Data Breach Security Act
S.C. Code Ann. §§ 39-1-90, *et seq.*

874. The South Carolina Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

875. Samsung is a business that owns, licenses, or maintains computerized data or other data that includes personal identifying information (for the purpose of this count, "PII"), as defined by S.C. Code Ann. § 39-1-90(A).

876. Plaintiff's and South Carolina Subclass Members' PII includes personal identifying information as covered under S.C. Code Ann. § 39-1- 90(D)(3).

877. Samsung is required to accurately notify Plaintiff and South Carolina Subclass Members following discovery or notification of a breach of its data security system if PII that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A) and (B).

878. Because Samsung discovered a breach of its data security system in which PII that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Samsung had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A) and (B).

879. By failing to disclose the Data Breach in a timely and accurate manner, Samsung violated S.C. Code Ann. § 39-1-90(A) and (B).

880. As a direct and proximate result of Samsung's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and South Carolina Subclass Members suffered damages, as described above.

881. Plaintiff and South Carolina Subclass Members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages, injunctive relief, and attorneys' fees.

COUNT 55
South Carolina Unfair Trade Practices Act
S.C. Code Ann. §§ 39-5-10, *et seq.*

882. The South Carolina Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

883. Samsung is a "person," as defined by S.C. Code Ann. § 39-5-10(a).

884. South Carolina's Unfair Trade Practices Act prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

885. Samsung advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

886. Samsung engaged in unfair and deceptive acts and practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and

sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

887. Samsung's acts and practices had, and continue to have, the tendency or capacity to deceive.

888. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

889. Samsung intended to mislead Plaintiff and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

890. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

891. Samsung had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the PII in its possession, and the generally accepted professional standards. Such a duty is also implied by law due to the nature of the relationship between consumers – including Plaintiff and the South Carolina Subclass – and Samsung, because consumers are unable to fully protect their interests with regard to the PII in Samsung's possession, and placed trust and confidence in Samsung. Samsung's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Carolina Subclass that contradicted these representations.

892. Samsung's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Samsung's acts and practices offend established public policies that seek to protect consumers' PII and ensure that entities entrusted with PII use appropriate

security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45; and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, *et seq*.

893. Samsung's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of Samsung's long history of inadequate data security and previous data breaches; the sensitivity and extent of PII in its possession; its special role as a linchpin of the financial system; and its admitted duty of trustworthiness and care as an entrusted protector of data.

894. Samsung's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Samsung engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including many South Carolinians impacted by the Data Breach, nearly half the state's population.

895. Samsung's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including numerous past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Samsung's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

896. Samsung's violations present a continuing risk to Plaintiff and South Carolina Subclass Members as well as to the general public.

897. Samsung intended to mislead Plaintiff and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

898. Samsung acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and South Carolina Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security

and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct, and would deter Samsung and others from committing similar conduct in the future.

As a direct and proximate result of Samsung's unfair and deceptive acts or practices, Plaintiff and South Carolina Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

899. Plaintiff and South Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 56
Tennessee Personal Consumer Information Act
Tenn. Code Ann. §§ 47-18-2107, *et seq.*

900. The Tennessee Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

901. Samsung is a business that conducts business in Tennessee and owns or licenses computerized personal information, as "personal information" is defined by Tenn. Code Ann. § 47- 18-2107(a)(4) (for the purpose of this count, "PII"), of residents of Tennessee and thus is an "Information holder" as defined by Tenn. Code Ann. § 47- 18-2107(a)(3).

902. Plaintiffs' and Tennessee Subclass Members' PII include PII as covered under Tenn. Code Ann. § 47-18- 2107(a)(4).

903. The Data Breach was a "breach of system security" as defined by Tenn. Code Ann. § 47-18-2107(a)(1).

904. Because Samsung discovered a breach of system security in which PII was, or is reasonably believed to have been, acquired by an unauthorized person, Samsung had an obligation to disclose the Data Breach as mandated by Tenn. Code Ann. § 47-18-2107(b) and (c).

905. By failing to disclose the Data Breach in a timely and accurate manner, Samsung violated Tenn. Code Ann. § 47-18-2107(b) and (c).

906. As a direct and proximate result of Samsung's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiffs and Tennessee Subclass Members suffered damages, as described above.

907. Samsung's violation of Tenn. Code Ann. § 47-18-2107(b) and (c) constitutes an unfair or deceptive act or practice affecting trade or commerce and subject to the penalties and remedies as provided in that Act, in addition to the penalties and remedies under Tenn. Code Ann. § 47-18-2107(b) and (c).

908. Plaintiffs and Tennessee Subclass Members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, treble damages, and reasonable attorneys' fees and costs.

COUNT 57
Tennessee Consumer Protection Act
Tenn. Code Ann. §§ 47-18-101, *et seq.*

909. The Tennessee Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

910. Samsung is a "person," as defined by Tenn. Code § 47-18-103(13).

911. Plaintiffs and Tennessee Subclass Members are "consumers," as meant by Tenn. Code § 47-18-103(2).

912. Samsung advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

913. Samsung advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And Samsung's acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

914. Samsung's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties

pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

915. Samsung intended to mislead Plaintiff and Tennessee Subclass Members and induce them to rely on its misrepresentations and omissions.

916. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

917. Had Samsung disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

918. Samsung had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the PII in its possession, and the generally accepted professional standards. In addition, such a duty is implied by law due to the nature of the relationship between

consumers, including Plaintiffs and Tennessee Subclass Members, and Samsung because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Samsung. Samsung's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and Tennessee Subclass that Members contradicted these representations.

919. Samsung's "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

920. The injury to consumers was and is substantial because it was non-trivial and non-speculative, and involved a monetary injury and/or an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

921. Consumers could not have reasonably avoided injury because Samsung's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Samsung created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

922. Samsung's inadequate data security had no countervailing benefit to consumers or

to competition.

923. By misrepresenting and omitting material facts about its data security and failing to comply with its common law and statutory duties pertaining to data security (including its duties under the FTC Act), Samsung violated the following provisions of Tenn. Code § 47-18- 104(b):

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve.

924. Samsung acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiffs and Tennessee Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

925. As a direct and proximate result of Samsung's unfair and deceptive acts or practices, Plaintiffs and Tennessee Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

926. Samsung's violations present a continuing risk to Plaintiffs and Tennessee Subclass Members as well as to the general public.

927. Plaintiffs and Tennessee Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 58
Deceptive Trade Practices-Consumer Protection Act
Texas Bus. & Com. Code § 17.41, *et seq.*

928. The Texas Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

929. Samsung is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

930. Plaintiff and the Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

931. Samsung advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

932. Samsung engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised;

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

933. Samsung's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

934. Samsung intended to mislead Plaintiff and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

935. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

936. Had Samsung disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. Samsung accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

937. Samsung had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and Texas Subclass Members, and Samsung because consumers are unable to

fully protect their interests with regard to their data, and placed trust and confidence in Samsung. Samsung's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and Texas Subclass Members that contradicted these representations.

938. Samsung engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Samsung engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

939. Consumers, including Plaintiff and Texas Subclass Members, lacked knowledge about deficiencies in Samsung's data security because this information was known exclusively by Samsung. Consumers also lacked the ability, experience, or capacity to secure the PII in Samsung's possession or to fully protect their interests with regard to their data. Plaintiff and Texas Subclass Members lack expertise in information security matters and do not have access to Samsung's systems in order to evaluate its security controls. Samsung took advantage of its special skill and access to PII to hide its inability to protect the security and confidentiality of Plaintiff's and Texas Subclass Members' PII.

940. Samsung intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Samsung's conduct is glaringly noticeable, flagrant,

complete, and unmitigated. The Data Breach, which resulted from Samsung's unconscionable business acts and practices, exposed Plaintiff and Texas Subclass Members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiff and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

941. Samsung acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

942. As a direct and proximate result of Samsung's unconscionable and deceptive acts or practices, Plaintiff and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach. Samsung's unconscionable and deceptive acts or practices were a producing cause of Plaintiff's and Texas Subclass Members' injuries, ascertainable losses, economic damages, and non- economic damages, including their mental anguish.

943. Samsung's violations present a continuing risk to Plaintiff and Texas Subclass Members as well as to the general public.

944. As set forth in paragraphs 420-421 above, Plaintiff has substantially complied with the notice requirements of Tex. Bus. & Com. Code § 17.505. In addition, Samsung received written

notice of the factual bases of this cause of action and others when plaintiffs in multiple actions that were filed in multiple jurisdictions served Samsung with complaints in connection with the Data Breach. Those complaints were filed more than 90 days ago, prior to the consolidation of the actions in the United States District Court for the District of New Jersey.[66]

945. These actions contained similar factual allegations to those giving rise to this cause of action, and Samsung has therefore had ample opportunity to investigate the basis of this action and pursue settlement discussions.

946. To date, Samsung has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiff's counsel.

947. Contemporaneous with the filing of this Consolidated Complaint, pursuant to Tex. Bus. & Com. Code Ann. § 17.501, Plaintiff's counsel will send to the Consumer Protection Division a copy of the written notice sent to Samsung.

948. Plaintiff and Texas Subclass Members seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT 59
Washington Data Breach Notice Act
Wash. Rev. Code §§ 19.255.010, *et seq.*

949. The Washington Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Washington Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth

[66] *See* note 61, *supra.*

herein.

950. Samsung is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by Wash. Rev. Code § 19.255.010(1), and maintains or possesses data that may include PII that Samsung does not own or license.

951. Plaintiffs' and Washington Subclass Members' PII includes PII as defined by Wash. Rev. Code § 19.255.005(2) and covered under Wash. Rev. Code § 19.255.010(1) and (2).

952. Samsung is required to accurately notify Plaintiffs and Washington Subclass Members following discovery or notification of the breach of its data security system if PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code §§ 19.255.010(1), (2), and (8).

953. Because Samsung discovered a breach of its security system in which PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, Samsung had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010, including by identifying in the notice the types of PII that were subject to the breach.

954. By failing to disclose the Data Breach in a timely and accurate manner and failing to provide the information required, Samsung violated Wash. Rev. Code § 19.255.010(1), (2), and (8).

955. As a direct and proximate result of Samsung's violations of Wash. Rev. Code § 19.255.010(1), (2), and (8), Plaintiffs and Washington Subclass Members suffered damages, as described above.

956. Plaintiffs and Washington Subclass Members seek relief under Wash. Rev. Code §§ 19.255.040(3)(a) and 19.255.040(3)(b), including actual damages and injunctive relief.

COUNT 60
Washington Consumer Protection Act
Wash. Rev. Code §§ 19.86.020, *et seq.*

957. The Washington Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Washington Subclass, repeat and re-allege the factual allegations set forth in paragraphs 1 through 268 above and incorporate the same as if set forth herein.

958. Samsung is a "person," as defined by Wash. Rev. Code § 19.86.010(1).

959. Samsung advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code § 19.86.010 (2).

960. Samsung engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

961. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

962. Samsung acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

963. Samsung's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and has the capacity to injure persons. Further, its conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

964. As a direct and proximate result of Samsung's unfair methods of competition and

unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

965. Plaintiffs and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS

COUNT 61
Wisconsin Deceptive Trade Practices Act
Wis. Stat. § 100.18

966. The Wisconsin Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 268 above and incorporates the same as if set forth herein.

967. Samsung is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

968. Plaintiff and Wisconsin Subclass Members are members of "the public," as defined by Wis. Stat. § 100.18(1).

969. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Samsung to members of the public for sale, use, or distribution, Samsung made, published, circulated, placed before the public or caused (directly or indirectly) to be made,

published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100. Samsung also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

970. Samsung's deceptive acts, practices, plans, and schemes include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Wisconsin data breach statute, Wis. Stat. §§ 134.98(2), *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Wisconsin data breach statute, Wis. Stat. §§

134.98(2), *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Wisconsin data breach statute, Wis. Stat. §§ 134.98(2), *et seq.*

971. Samsung intended to mislead Plaintiff and Wisconsin Subclass Members and induce them to rely on its misrepresentations and omissions.

972. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

973. Samsung had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers – including Plaintiff and Wisconsin Subclass Members – and Samsung, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Samsung. Samsung's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from

Plaintiff and Wisconsin Subclass Members that contradicted these representations.

974. Samsung's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

975. Samsung acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

976. As a direct and proximate result of Samsung's deceptive acts or practices, Plaintiff and Wisconsin Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

977. Samsung had an ongoing duty to its customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

978. Plaintiff and Wisconsin Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

REQUEST FOR RELIEF

979. Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Samsung, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead Interim Class Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Samsung from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

1. Requiring Samsung to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII;

2. Requiring Samsung to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct automated security monitoring and testing, including simulated attacks, penetration tests, and audits on Samsung systems on a periodic basis, and ordering Samsung to promptly correct any problems or issues detected by such third-party security auditors; protect all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

3. Requiring Samsung to delete, destroy and purge the PII of Plaintiffs and Class Members unless Samsung can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

4. Requiring Samsung to audit, test, and train their security personnel regarding any new or modified procedures;

5. Requiring Samsung to segment data by, among other things, creating firewalls and access controls so that if one area of Samsung's network is compromised, hackers

cannot gain access to other portions of Samsung's systems;

6. Requiring Samsung to conduct regular database scanning and securing checks;

7. Requiring Samsung to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

8. Requiring Samsung to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

9. Requiring Samsung to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Samsung's policies, programs and systems for protecting PII;

10. Requiring Samsung to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor Samsung's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

11. Requiring Samsung to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

12. Requiring Samsung to implement logging and monitoring programs sufficient to track traffic to and from Samsung servers;

13. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis Samsung's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment; and

14. Prohibiting Samsung from engaging in the wrongful and unlawful acts described herein.

C. That the Court award Plaintiffs and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Samsung as a result of its unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiffs be granted the declaratory relief sought herein;

G. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

980. Plaintiffs demand a jury trial on all claims so triable.

DATED: July 14, 2023

Respectfully submitted,

/s/ James E. Cecchi

James E. Cecchi
Caroline F. Bartlett
CARELLA BYRNE CECCHI BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ07068
Tel. (973) 994-1700

Ryan J. Clarkson
Yana A. Hart
CLARKSON LAW FIRM, P.C.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel. (213) 788-4050

Linda P. Nussbaum
NUSSBAUM LAW GROUP, P.C.
1211 Avenue Of The Americas
40th Floor
New York, NY 10036-8718
Tel. (917) 438-9189

Roberta D. Liebenberg
Mary L. Russell
FINE, KAPLAN & BLACK
One S. Broad Street
23rd Floor
Philadelphia, PA 19107
Tel. (215) 567-6565

Catherine B. Derenze
LITE DEPALMA GREENBERG & AFANADOR, LLC
570 Broad Street, Suite 1201
Newark, NJ 07102
Tel. (973) 623-3000

Kelly Iverson
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel. (412) 322-9243

Christopher A. Seeger
Christopher L. Ayers
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, NJ 07660
Tel. (973) 639-9100

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street
14th Floor
New York, NY 10004
Tel. (646) 357-1100

Sabita J. Soneji
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, California 94612
Tel. (510) 254-6808

Nada Djordjevic
DICELLO LEVITT LLC
Ten North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
Tel. (312) 214-7900

Attorneys for Plaintiffs and Members of the Leadership Committee